

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire GEM 362	POUR SUITE A DONNER voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
Demande internationale n° PCT/FR 98/ 00582	Date du dépôt international (jour/mois/année) 20/03/1998	(Date de priorité (la plus ancienne) (jour/mois/année) 11/04/1997
Déposant GEMPLUS S.C.A et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

☒ Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. ☐ Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche (voir le cadre I).
2. ☐ Il y a absence d'unité de l'invention (voir le cadre II).
3. ☐ La demande internationale contient la divulgation d'un **listage de séquence de nucléotides ou d'acides aminés** et la recherche internationale a été effectuée sur la base du listage de séquence
 - ☐ déposé avec la demande internationale
 - ☐ fourni par le déposant séparément de la demande internationale
 - ☐ sans être accompagnée d'une déclaration selon laquelle il n'inclut pas d'éléments allant au-delà de la divulgation faite dans la demande internationale telle qu'elle a été déposée.
 - ☐ transcrit par l'administration
4. En ce qui concerne le titre, ☒ le texte est approuvé tel qu'il a été remis par le déposant.
☐ Le texte a été établi par l'administration et a la teneur suivante:
5. En ce qui concerne l'abrégé,
 - ☒ le texte est approuvé tel qu'il a été remis par le déposant
 - ☐ le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.
6. La figure **des dessins** à publier avec l'abrégé est la suivante:
 Figure n° 2 ☒ suggérée par le déposant. ☐ Aucune des figures n'est à publier.
 - ☐ parce que le déposant n'a pas suggéré de figure.
 - ☐ parce que cette figure caractérise mieux l'invention.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No

PCT/FR 98/00582

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 G07F17/32 G07F7/08

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 6 G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	WO 93 17403 A (NSM) 2 septembre 1993 voir abrégé; revendications 13-24; figures voir page 6, alinéa 2 - page 9, alinéa 1 ---	1-5, 16, 23
Y	DE 44 27 039 A (GIESECKE & DEVRIENT) 1 février 1996 voir abrégé; revendications; figures 1, 2 voir colonne 3, ligne 32 - colonne 4, ligne 41 ---	1-5, 16, 23
A	EP 0 589 545 A (BALLY GAMING INTERNATIONAL) 30 mars 1994 voir abrégé; revendications; figure voir colonne 4, ligne 8 - colonne 8, ligne 56 --- -/-	1-6, 16, 23



Voir la suite du cadre C pour la fin de la liste des documents



Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

21 juillet 1998

Date d'expédition du présent rapport de recherche internationale

31/07/1998

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,

Fonctionnaire autorisé

David. J

RAPPORT DE RECHERCHE INTERNATIONALE

Requête internationale No

PCT/FR 98/00582

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 96 08798 A (GEMPLUS) 21 mars 1996 voir abrégé; revendications; figures ----	1,2,6-23
A	EP 0 762 333 A (TEXAS INSTRUMENTS) 12 mars 1997 ----	
A	EP 0 619 564 A (PITNEY BOWES) 12 octobre 1994 ----	
A	WO 97 02547 A (KONINKLIJKE PTT NEDERLAND) 23 janvier 1997 -----	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 98/00582

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 9317403	A	02-09-1993	DE 4205791 A	02-09-1993
			AT 132992 T	15-01-1996
			DE 59301417 D	22-02-1996
			EP 0628192 A	14-12-1994
			US 5557086 A	17-09-1996
DE 4427039	A	01-02-1996	EP 0696021 A	07-02-1996
EP 0589545	A	30-03-1994	US 5371345 A	06-12-1994
			AU 660561 B	29-06-1995
			AU 4623393 A	24-03-1994
			CA 2105925 A	18-03-1994
WO 9608798	A	21-03-1996	FR 2724748 A	22-03-1996
			AU 3475695 A	29-03-1996
			ZA 9507809 A	07-05-1996
EP 0762333	A	12-03-1997	JP 9297862 A	18-11-1997
EP 0619564	A	12-10-1994	US 4802218 A	31-01-1989
			EP 0619563 A	12-10-1994
			EP 0619565 A	12-10-1994
			AT 116778 T	15-01-1995
			AT 160456 T	15-12-1997
			AT 160039 T	15-11-1997
			AU 605443 B	10-01-1991
			AU 7961287 A	24-03-1988
			CA 1320578 A	20-07-1993
			CA 1326911 A	08-02-1994
			CA 1335839 A	06-06-1995
			CA 1296809 A	03-03-1992
			DE 3750958 D	16-02-1995
			DE 3750958 T	08-06-1995
			DE 3752138 D	11-12-1997
			DE 3752138 T	26-03-1998
			DE 3752146 D	02-01-1998
			DE 3752146 T	09-04-1998
			DK 228888 A	17-06-1988
			EP 0294397 A	14-12-1988
			EP 0740275 A	30-10-1996

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 98/00582

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0619564 A		FI 882047 A,B,	02-05-1988
		JP 1500863 T	23-03-1989
		JP 2661932 B	08-10-1997
		NO 300660 B	30-06-1997
		WO 8801818 A	10-03-1988
		US 4864618 A	05-09-1989
		US 4900904 A	13-02-1990
		US 4900903 A	13-02-1990
WO 9702547 A	23-01-1997	NL 1000741 C	08-01-1997
		AU 6613096 A	05-02-1997
		EP 0836730 A	22-04-1998
		NO 976151 A	03-03-1998

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

United States Patent and Trademark
Office
(Box PCT)
Crystal Plaza 2
Washington, DC 20231
ÉTATS-UNIS D'AMÉRIQUE

en sa qualité d'office élu

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Date d'expédition (jour/mois/année) 29 décembre 1998 (29.12.98)	
Demande internationale no PCT/FR98/00582	Référence du dossier du déposant ou du mandataire GEM 362
Date du dépôt international (jour/mois/année) 20 mars 1998 (20.03.98)	Date de priorité (jour/mois/année) 11 avril 1997 (11.04.97)
Déposant ORUS, Hervé etc	

1. L'office désigné est avisé de son élection qui a été faite:



dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

16 novembre 1998 (16.11.98)



dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection ☐ a été faite

n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur: (41-22) 740.14.35

Fonctionnaire autorisé

Jocelyne Rey-Millet

no de téléphone: (41-22) 338.83.38

PCT

ORGANISATION MONDIALE DE LA PROPRIÉTÉ INTELLECTUELLE
Bureau international

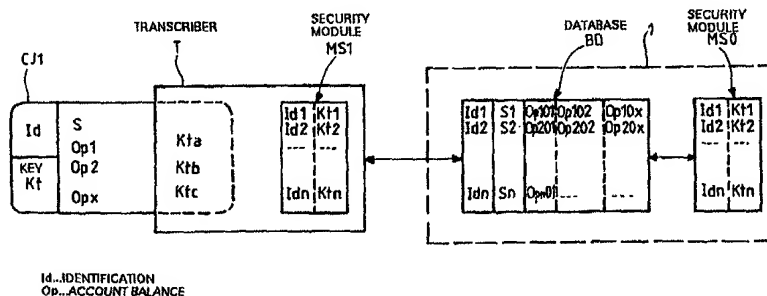


DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIÈRE DE BREVETS (PCT)

(51) Classification internationale des brevets ⁶ : G07F 17/32, 7/08	A1	(11) Numéro de publication internationale: WO 98/47113 (43) Date de publication internationale: 22 octobre 1998 (22.10.98)
(21) Numéro de la demande internationale: PCT/FR98/00582 (22) Date de dépôt international: 20 mars 1998 (20.03.98) (30) Données relatives à la priorité: 97/04733 11 avril 1997 (11.04.97) FR (71) Déposant (pour tous les Etats désignés sauf US): GEMPLUS S.C.A. [FR/FR]; Avenue du Pic de Bertagne, Parc d'activités de Gémenos, F-13881 Gémenos Cedex (FR). (72) Inventeurs; et (75) Inventeurs/Déposants (US seulement): ORUS, Hervé [FR/FR]; 20, rue de la Grafontaine, Zac Lou Caire, F-13470 Carnoux en Provence (FR). FOGLINO, Jean-Jacques [FR/FR]; Les Terrasses de l'Audiguier, F-13790 Peynier (FR). (74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A., Z.I. Athelia III, Voie Antiope, F-13705 La Ciotat Cedex (FR).		(81) Etats désignés: AU, BR, CA, CN, JP, KR, MX, RU, SG, US, VN, brevet européen (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Publiée Avec rapport de recherche internationale.

(54) Title: SECURITY PROCEDURE FOR CONTROLLING THE TRANSFER OF VALUE UNITS IN A CHIP CARD GAMING SYSTEM

(54) Titre: PROCEDURE SECURISEE DE CONTROLE DE TRANSFERT D'UNITES DE VALEUR DANS UN SYSTEME DE JEU A CARTES A PUCE



(57) Abstract

The invention concerns slot machines, such as jackpot or black jack and other casino gambling machines. The machines are designed to operate with gaming cards (CJ1), such as chip cards, and are connected by network to a central management unit (1). The invention is characterised in that the central management unit comprises a database (BD), wherein are stored data corresponding to those stored on the gaming cards such data concerning the gamester and card identification data (Id) and data (S, Op1, Op2) concerning the account balance stored in the card (CJ1). The procedure consists in verifying the card data with respect to the central management unit database to ensure the integrity of such a gambling machine system operating with chip cards or contactless cards.

(57) Abrégé

L'invention concerne les machines à sous, type jack-pot, black-jack, et autres machines de jeu d'argent de casino. Il est prévu que les machines de jeu fonctionnent avec des cartes de jeu (CJ1), type carte à puce, et sont reliées en réseau avec un organe central de gestion (1). L'invention prévoit que l'organe central de gestion comporte une base de données (BD), dans laquelle sont stockées des informations correspondantes à celles stockées sur les cartes de jeu comme des informations sur le joueur ainsi que des données (Id) d'identification des cartes et des données (S, Op1, Op2) renseignant sur le solde de la valeur stockée dans la carte (CJ1). Une vérification des données de la carte par rapport aux données de la base de l'organe central de gestion permet d'assurer l'intégrité d'un tel système de machines de jeu fonctionnant avec des cartes à puce ou des cartes sans contact.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce	ML	Mali	TR	Turquie
BG	Bulgarie	HU	Hongrie	MN	Mongolie	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MR	Mauritanie	UA	Ukraine
BR	Brésil	IL	Israël	MW	Malawi	UG	Ouganda
BY	Biélorus	IS	Islande	MX	Mexique	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	NE	Niger	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NL	Pays-Bas	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norvège	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NZ	Nouvelle-Zélande	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	PL	Pologne		
CM	Cameroun	KR	République de Corée	PT	Portugal		
CN	Chine	KZ	Kazakhstan	RO	Roumanie		
CU	Cuba	LC	Sainte-Lucie	RU	Fédération de Russie		
CZ	République tchèque	LI	Liechtenstein	SD	Soudan		
DE	Allemagne	LK	Sri Lanka	SE	Suède		
DK	Danemark	LR	Liberia	SG	Singapour		
EE	Estonie						

PROCEDURE SECURISEE DE CONTROLE DE TRANSFERT D'UNITES
DE VALEUR DANS UN SYSTEME DE JEU A CARTE A PUCE

5 La présente invention concerne le domaine des machines à sous, telles que les dispositifs de jack-pot et les autres dispositifs de jeux d'argent individuels du type de ceux que l'on trouve dans les casinos.

10 Elle concerne plus particulièrement des machines à sous permettant d'enregistrer des mises et des gains avec des cartes de jeu. Les cartes de jeu sont du type carte à puce ou carte sans contact. Les cartes de jeu peuvent être dédiées à cette utilisation suivant l'exemple des cartes téléphoniques. Elles sont
15 avantageusement constituées par des cartes bancaires, permettant de transférer des sommes d'argent directement sur la machine à sous.

La présente demande vise un procédé et un système de contrôle de transfert d'unités de valeur entre une pluralité de cartes de jeu et une pluralité de machines
20 de jeu, chaque machine étant connectée à un transcripteur de données sur cartes de jeu apte à créditer et/ou à débiter des unités de valeur en mémoire d'une carte de jeu.

Un objectif général du contrôle de transfert
25 d'unités de valeurs entre cartes de jeu et machines de jeu est d'éviter toute malversation financière à l'aide de telle cartes.

On connaît déjà des systèmes de gestion pour des machines de jeu équipées de lecteurs de cartes à puce,
30 adaptés à la gestion d'un parc de machines de jeux disposées dans des sites relativement fermés et contrôlés comme les casinos. Ces systèmes sont adaptés à un tel environnement, car il font l'objet de contrôles et de réglementations importants, peu

susceptibles de permettre des fraudes sur les transactions de jeux utilisant des cartes à puce.

Le document EP-A-0 360 613 décrit par exemple un système de transfert de données entre carte à puce et une pluralité de machines avec des moyens de transmission et de stockage des données machine dans la carte à puce. Un tel système permet d'effectuer un relevé des opérations de jeu avec une carte de collecte stockant une liste des opérations de jeux effectuées dans un but comptable ou fiscal.

Un inconvénient d'un tel système est qu'on ne peut pas contrôler toutes les opérations de jeu effectuées, sauf à relever toutes les machines avec la carte de collecte, ce qui occasionne des manipulations fastidieuses.

D'autre part, devant la demande croissante du public, il est envisagé d'installer des machines de jeu dans des sites moins protégés que les casinos comme des salles de jeux privées ou des bars, voire même dans des lieux d'habitation privés comme le domicile des joueurs.

Il apparaît clairement qu'une telle dispersion des machines de jeu pose d'importants problèmes de sécurité des transactions suite aux opérations de jeu.

Un but de l'invention est de permettre un développement des machines de jeu fonctionnant avec des cartes à puce dans des lieux non protégés.

Un autre but de l'invention est de renforcer l'intégrité des systèmes de machines de jeux fonctionnant avec des cartes de jeu.

L'invention prévoit que les machines de jeu sont reliées en réseau avec un organe central de gestion. Selon l'invention on a prévu que l'organe central de gestion comporte une base de données, dans laquelle

5 sont stockées des informations correspondantes à celles
stockées sur les cartes de jeu comme des informations
sur le joueur ainsi que des données d'identification
des cartes et des données renseignant sur le solde de
la valeur stockée dans la carte. Une vérification des
données de la carte par rapport aux données de la base
de l'organe central de gestion permet d'assurer
l'intégrité d'un tel système de machines de jeu
fonctionnant avec des cartes à puce ou des cartes sans
10 contact.

L'invention prévoit ainsi un procédé sécurisé de
contrôle de transferts d'unités de valeur entre une
pluralité de cartes de jeu et une pluralité de machines
de jeu, chaque machine étant connectée à un
15 transcripteur de données sur carte de jeu, les machines
étant reliées en réseau sécurisé avec un organe central
de gestion par l'intermédiaire de moyens de liaison, le
procédé comportant des étapes consistant, au cours
d'une opération de jeu, à :

20 - lire des données en mémoire d'une carte de jeu,
notamment un numéro d'identification de la carte et des
données représentatives des unités de valeur débitées
et/ou créditées au cours des opérations de jeu
précédentes,

25 - échanger des données entre la machine et une base
de données de l'organe central de gestion par
l'intermédiaire des moyens de liaison du réseau
sécurisé, notamment des données représentatives de
solde des unités de valeur et/ou le numéro
30 d'identification de la carte ; et,

- vérifier que les données en mémoire de la carte
de jeu correspondent aux données de la base de données
afin de contrôler l'intégrité d'un système constitué

par une telle carte, une telle machine, le réseau et l'organe central de gestion.

5 L'invention prévoit avantageusement des moyens de sécurisation qui permettent d'authentifier les messages de données échangées sur le réseau, c'est-à-dire de signer de tels messages.

10 L'invention prévoit en outre un système sécurisé de contrôle de transferts d'unités de valeur entre une pluralité de cartes de jeu et une pluralité de machines de jeu, chaque machine étant pourvue d'un transcripteur apte à débiter des unités de valeur d'une carte de jeu, les machines étant reliées en réseau sécurisé avec un organe central de gestion par l'intermédiaire de moyens de liaison, une carte de jeu stockant en mémoire des données représentatives d'opérations de jeu effectuées, 15 notamment des données d'identification de la carte et des données représentatives de solde des valeurs débitées et/ou créditées au cours des opérations de jeu précédentes, caractérisé en ce que l'organe central de gestion comporte une base de données stockant 20 parallèlement en mémoire les données représentatives des opérations de jeu effectuées, notamment les données d'identification des cartes et les données représentatives des soldes des valeurs débitées et/ou 25 créditées au cours des opérations de jeu précédentes et en ce que des moyens de contrôle vérifient que, pour une carte identifiée, les données de la base et les données de la carte correspondent, notamment que les données représentatives du solde correspondent, afin de 30 vérifier l'intégrité du système.

Un module de sécurisation pour l'authentification des messages de données peut avantageusement être prévu dans le réseau, au niveau d'un transcripteur, d'une

machine, de l'organe central, ou même des moyens de liaison du réseau.

L'invention sera mieux comprise à la lecture de la description et des dessins qui suivent, donnés
5 uniquement à titre d'exemples non limitatifs ; sur les dessins annexés :

- la figure 1 représente un système sécurisé de contrôle de transfert d'unités de valeurs entre une pluralité de cartes de jeu et une pluralité de machines
10 de jeu apte à mettre en oeuvre l'invention ;

- la figure 2 représente un schéma d'échange et de vérification des données selon l'invention ; et,

- la figure 3 représente un calcul de certificat d'authentification par des moyens de sécurisation selon
15 l'invention.

Sur la figure 1 on a représenté un système sécurisé de machines de jeu tel que proposé par l'invention, et qui comprend une ou plusieurs machines de jeu 200, 200', 200" et 200'''.

20 Une telle machine de jeu 200, semblable aux machines à sous que l'on trouve dans les casinos dispose d'un monnayeur électronique 210 que l'on appellera par la suite transcripteur de données sur carte de jeu CJ.

25 Le transcripteur de données sur carte 210 est relié à l'électronique de la machine 200, par exemple par une liaison série de type RS 485. La machine et le lecteur comportent des interfaces entrée-sortie adaptées à cette liaison.

30 De façon classique, la machine est équipée d'un écran d'affichage 211 qui permet aux joueurs de savoir à tout instant quel est le solde dont il dispose pour jouer et le montant des mises et des gains réalisés.

La machine 200 qui a été représentée peut bien sûr être une machine à monnayeur électronique exclusivement, mais aussi une machine à double monnayeur, c'est-à-dire une machine qui comporte outre
5 ce monnayeur électronique, un monnayeur à pièces (ou à jetons) symbolisé par la référence 201.

Dans le cas d'une machine à double monnayeur, le joueur aura la possibilité de jouer avec des pièces ou jetons et de se faire restituer ses gains uniquement
10 sous la forme de pièces.

Les cartes de jeu CJ représentées sous forme de cartes à puce comportent une mémoire morte effaçable électriquement, par exemple une mémoire de type EEPROM.

Il peut s'agir également de cartes à puce
15 comportant un microprocesseur, une mémoire de programmes et une mémoire de travail de type RAM.

Ces cartes à puce peuvent également être des cartes à chargement d'unités de type rechargeable. Ces cartes comportent pour cela une mémoire électriquement
20 programmable du genre boulier.

En outre les cartes de jeu peuvent être constituées par des cartes sans contact, la carte comportant un circuit intégré à mémoire et microprocesseur, et un circuit électronique de transmission de données sans
25 contact électrique. On peut par exemple utiliser un transpondeur tel que décrit dans la demande de brevet FR - 96 16061.

La réalisation des machines de jeu 200 et leur connexion à des transpositeurs de données sur cartes de
30 jeu ne sera pas détaillée ici. Des exemples de réalisations de machines de jeu sont détaillés par exemple dans la demande de brevet FR - 96 10031 dont la description est incorporée à la présente.

Afin de contrôler les opérations de jeux et les transactions avec les cartes, il est prévu de relier les machines 200, 200', 200", 200''' en réseau, avec un organe central de gestion représentés sous la référence 1 à la figure 1. Les machines du réseau sont reliées à l'organe central de gestion 1 par des moyens de liaison 123. Comme représentées à la figure 1, les machines 200, 200', 200", 200''' peuvent également être reliées entre elles par le réseau.

Les moyens de liaison 123 sont constitués dans le cas d'un réseau local comme celui d'un casino par une liaison locale. La liaison locale est par exemple une liaison série de type RS 485, un bus de liaison parallèle, une fibre optique, une liaison radio ou tout autre support de transmission.

Dans le cas d'un réseau joignant des salles de jeu dispersées, les moyens de liaisons peuvent être constitués par des canaux de transmission propres au réseau ou par des lignes téléphoniques.

Pour établir des liaisons téléphoniques, le réseau comporte des modulateurs-démodulateurs de type MODEM 120, 120', 120" et 120''', disposés en interface entre les moyens de liaison 123 et une machine de jeux 200, 200', 200", 200''' respectivement.

L'organe central de gestion 1 est constitué par exemple d'un ordinateur central relié également aux moyens de liaison 123 par un MODEM 101 de façon à faire partie du réseau.

Sur la figure 1 on a représenté des moyens de liaison 123 sous la forme schématique d'une ligne annulaire à laquelle les machines de jeux 200, 200', 200" et 200''' sont connectées. Les machines sont ainsi reliées entre elles et à l'organe central de gestion 1.

La liaison peut cependant prendre toutes sortes de formes équivalentes.

Dans le cas de liaisons téléphoniques, les machines sont reliées individuellement aux moyens centralisés de gestion, les machines n'étant pas nécessairement reliées entre elles. Le MODEM 101 des moyens de gestion 1 peut comporter avantageusement un standard de plusieurs lignes téléphoniques.

L'utilisation de liaisons téléphoniques présente l'avantage de permettre d'étendre le réseau au lieu d'habitation des joueurs. Les machines de jeux sont de préférence constituées par des ordinateurs personnels 300 et 300' de type PC. Les machines peuvent ainsi être connectées chacune à un transcripteur de données sur carte de jeu 310 ou 310' intégrant de préférence un MODEM 130 ou 130', par exemple du type "GEMTEL" commercialisé par la demanderesse.

Le réseau utilisé peut être notamment un réseau de communication ouvert du type "INTERNET".

Il est prévu en outre que le système et le réseau comportent au moins un terminal de chargement représenté à la figure 1 sous forme d'une caisse enregistreuse 100. Le terminal de chargement 100 comporte alors un transcripteur 110. Le terminal 100 et le transcripteur 110 sont alors reliés au réseau par l'intermédiaire d'un MODEM 111 connecté aux moyens de liaison 123.

Classiquement, il est prévu que les cartes à puce dédiées aux jeux sont des cartes non-rechargeables, à l'instar des cartes téléphoniques, et elles sont fabriquées et chargées uniquement par un organisme central.

Dans une application avec des cartes non-rechargeables, il est prévu que la base de données BD

des moyens centralisés de gestion 1 dispose des soldes S1, S2, ..., Sn initiaux des valeurs créditées sur les cartes CJ1, CJ2, ..., CJn avant leur mise en circulation.

5 Cependant, selon une variante avantageuse, il est prévu que les cartes sont rechargées en unités de valeurs par l'intermédiaire de terminaux de chargement.

10 En pratique, ce terminal peut être celui d'un caissier du casino. De façon alternative, on peut prévoir une multitude de terminaux de chargements disposés dans des débits de tabac ou dans d'autres commerces accessibles aux joueurs.

15 Ainsi lorsqu'un joueur désire obtenir la délivrance d'un crédit, il donne sa carte de jeu CJ1 à l'opérateur habilité à utiliser le terminal 100 qui insère cette carte dans la partie transcripteur 110 de ce terminal 100 et qui au moyen du clavier de la caisse va rentrer le montant du crédit que désire avoir le joueur. Ce montant est transféré au transcripteur 110 qui

20 enregistre alors sur la carte à puce CJ1 l'information significative correspondant au crédit désiré par le joueur.

25 Selon l'invention, le terminal de rechargement peut alors communiquer à l'organe central de gestion 1, par l'intermédiaire des moyens de liaison du réseau 123, les données lues sur la carte à recharger, notamment son numéro d'identification Id et son solde S d'unités de valeur. La vérification du numéro d'identification Id de la carte de jeu CJ1 peut être faite directement

30 par le terminal de rechargement 100 ou par son transcripteur de données 110 ou de manière alternative par l'organe central de gestion 1. L'invention prévoit ainsi une étape préliminaire aux opérations de jeu, consistant à inscrire dans la base de données de

l'organe central de gestion 1 et dans la mémoire d'une carte de jeu CJ1, des données représentatives d'une valeur de solde initial lors d'une opération préliminaire de chargement de la carte CJ1.

5 Selon la première alternative, il est prévu comme visible à la figure 2 que le terminal de rechargement ou son transcripteur T dispose des clefs d'identification secrètes Kt1, Kt2, ..., Ktn de toutes les cartes de jeu CJ1, CJ2, ..., CJn en circulation.
10 Ces clés secrètes sont de préférence stockées dans un module de sécurisation MS1 comportant une mémoire et une unité de calcul, les données stockées n'étant pas accessibles de l'extérieur. Le terminal 100 vérifie alors que l'identification Id1 de la carte à puce CJ1
15 est correcte avec la clef Kt1 correspondante, en appliquant un algorithme d'authentification ou de cryptage selon les méthodes connues.

 Selon la seconde alternative, cette authentification de la carte est effectuée au niveau de
20 l'organe central de gestion 1, les numéros d'identification Id1, Id2, ..., Idn et les clefs d'authentification correspondantes Kt1, Kt2, ..., Ktn étant stockées dans la base de données BD de l'organe central de gestion ou de préférence dans un module de
25 sécurité MS0 similaire à MS1. Cette seconde alternative présente l'avantage d'éviter toute dissémination des clefs d'authentification secrètes.

 L'invention prévoit en outre un échange de données entre le terminal et l'organe central de gestion
30 portant sur les données stockées dans la base de données de l'organe central de gestion 1. De préférence, cet échange de données est accompagné d'un certificat d'authentification. Un protocole de sécurisation permettant d'émettre de tels certificats

sera détaillé ci-après. Ce protocole évite
avantageusement qu'une machine parasite du réseau ne
crédite abusivement la base de donnée. Le terminal T
peut ainsi communiquer le solde S des valeurs débitées
5 et/ou créditées précédemment sur la carte de jeu CJ1 à
l'organe central de gestion 1. Après avoir authentifié
le numéro d'identification Id1 de la carte ou le
certificat accompagnant les données de solde, on peut
ainsi vérifier que le solde S inscrit en mémoire de la
10 carte de jeu CJ1 correspond bien au solde S1 stocké
dans la base de données BD. Si la vérification est
positive, il est prévu que l'organe central de gestion
1 émet un signal d'accord pour le rechargement de la
carte CJ1 par le terminal et le transcripteur T. En cas
15 de vérification négative, une procédure ou un signal
d'alerte peuvent être mis en oeuvre au niveau de
l'organe central de gestion 1, ou au niveau du terminal
de chargement. Dans un réseau de machines à sous de
casino par exemple, le caissier pourra être alerté par
20 le terminal de chargement afin de découvrir l'origine
d'un tel dysfonctionnement. Dans un réseau plus étendu,
on peut prévoir que la carte CJ1 soit avalée par le
transcripteur T du terminal afin d'enquêter sur le
dysfonctionnement.

25 On peut prévoir en outre que la base de données ou
la mémoire des cartes de jeu CJ comportent des
informations sur le joueur, par exemple sur son âge,
ses habitudes de jeu pour des applications de
fidélisation des joueurs, de remise de parties
30 gratuites, etc.

Nous allons présenter maintenant des protocoles de
contrôle de transferts d'unités de valeur au cours
d'opérations de jeu effectuées avec le procédé ou le
système selon l'invention.

Au début des opérations de jeu, le transcripteur de données sur carte 210 de la machine de jeu lit le numéro d'identification en mémoire de la carte de jeu CJ1. Comme exposé précédemment au vu de la figure 2, ce
5 numéro d'identification Id est de préférence authentifié par un module de sécurité MS1 prévu dans le transcripteur T. Le numéro Id peut éventuellement être communiqué à l'organe central de gestion 1 en vue d'authentifier la carte CJ1 avec la clef
10 d'identification Kt1 contenue dans le module de sécurité MS0. Cette étape d'identification est de préférence effectuée une seule fois pour plusieurs opérations de jeu avec la même carte sur la même machine, la machine ou le terminal mémorisant
15 éventuellement ce numéro d'identification Id pour les opérations suivantes.

A chaque opération de jeu suivante, le solde S des unités de valeur affecté au joueur est revu à la suite des mises ou des gains réalisés.

20 Selon un premier mode de réalisation de l'invention, il est prévu de communiquer simplement à l'organe central de gestion 1 des données relatives à l'opération de jeu effectuée, notamment le nouveau solde d'unités de valeur obtenu au cours de cette
25 opération de jeu. L'organe central de gestion 1 peut ainsi stocker la liste des opérations effectuées, sous forme d'une liste des crédits ou des débits successifs enregistrés sur la carte CJ1. Cette liste des
30 opérations Op101, Op102, ... , Op10x est par exemple enregistrée dans la base de données BD sous le numéro d'identification Id1 de la carte CJ1 en cours d'utilisation.

La recopie du solde S1 ou des opérations Op101, Op102, ... , Op10x dans la base de données BD de

l'organe central de gestion 1 sert alors à établir un relevé comptable des opérations ou à effectuer des vérifications fiscales. Un tel historique des opérations permet également lors d'une vérification d'une carte falsifiée de mesurer l'étendue de la fraude.

Selon un deuxième mode de réalisation de l'invention, il est prévu une étape supplémentaire consistant à vérifier que les données en mémoire de la carte CJ1 et les données de la base de données BD correspondent afin de contrôler l'intégrité d'un système constitué par une telle carte CJ1, une telle machine 200, le réseau 123 et l'organe central de gestion 1.

Deux types de vérification peuvent être prévues, la vérification pouvant porter sur le numéro d'identification Id ou sur le solde S de la carte.

La vérification du numéro d'identification Id1 de la carte CJ1 est effectuée avec une clé d'identification Kt1 comme on l'a vu précédemment. Selon ce deuxième mode de réalisation, le numéro d'identification Id est communiqué à l'organe central 1 via les moyens de liaison 123 du réseau. L'organe central 1 stocke les clés d'identification Kt1, Kt2, ..., Ktn des cartes CJ1, CJ2, ..., CJn en circulation, dans sa base de donnée BD ou de préférence dans un module de sécurisation MS0. Le module de sécurisation MS0 effectue ainsi les calculs d'identification en interne.

De plus, la vérification peut porter sur le solde d'unités de valeur de la carte CJ1. Dans ce cas, le transcripteur T lit sur la carte les données de solde S des unités de valeur et les envoie à l'organe central de gestion 1 par l'intermédiaire des moyens de liaison

du réseau 123. La vérification du solde S de la carte CJ1 est alors effectuée par rapport au solde S1 indiqué dans la base de données BD sous le numéro d'identification Id1. Si les deux soldes S et S1
5 correspondent, l'opération de jeu est autorisée par l'organe central de gestion 1.

Selon une autre alternative, la vérification peut porter sur la certification des données échangées à partir de la carte de jeu CJ1. Des algorithmes
10 standards d'encryptage de données type algorithme DES permettent en effet de certifier les données numériques échangées entre la carte CJ1, le transcripteur T, la machine de jeu et l'organe central de gestion 1. Le cryptage et le décryptage du certificat accompagnant
15 les données transmises n'est possible et cohérent que si on utilise une clé secrète.

Les algorithmes de cryptage de données de type DES comportent des séries de calculs complexes qui ne seront pas détaillés dans la présente.

20 Un exemple de mise en oeuvre d'algorithme DES sera exposé en considérant simplement que l'algorithme fournit un nombre crypté, appelé clef de session K', à partir d'un premier nombre donné, appelé clef d'identification K et d'un nombre aléatoire Rnd, selon
25 l'exemple de la formule suivante :

$$K' = \text{DES}(K, \text{Rnd})$$

La complexité des algorithmes DES rend impossible la découverte d'une clef d'identification secrète K à
30 partir de la clef de session K' et du nombre aléatoire Rnd.

La figure 3 montre un exemple d'application d'un algorithme DES. Il permet d'illustrer des moyens de sécurisation du réseau, en particulier la sécurisation

des échanges de données effectuées via les moyens de liaison du réseau. La carte de jeu dispose dans une zone mémoire inaccessible d'au moins une clé d'identification secrète K_t . Le microprocesseur de la
5 carte génère un nombre pseudo aléatoire $Rnd1$. A partir de ces deux nombres $Rnd1$ et K_t , l'algorithme DES mis en oeuvre par le microprocesseur calcule une clef de session K_t' .

Cette clef de session K_t' peut servir de certificat
10 d'authentification et être envoyée avec le nombre aléatoire $Rnd1$ et les données à certifier. Cependant, pour rendre toute découverte des clefs impossible, il est prévu d'appliquer une seconde fois l'algorithme DES. Comme visible figure 3, la carte de jeu, organe
15 émetteur du message à certifier, demande à l'organe destinataire, l'organe central 1 par exemple, de lui fournir un second nombre aléatoire $Rnd2$.

L'algorithme DES est à nouveau appliqué à la clef de session K_t' et au second nombre aléatoire $Rnd2$ par
20 le microprocesseur de la carte pour calculer un certificat C.

Le message de données est alors envoyé à l'organe destinataire accompagné du certificat C et du nombre aléatoire $Rnd1$ calculés par la carte. Ainsi les clefs
25 utilisées, en particulier la clef d'identification secrète K_t , ne sont pas échangées.

L'authentification du message de données est effectué en recalculant un certificat C' à partir des
30 mêmes données. L'organe central de gestion 1 dispose dans son module sécurisé MSO de la clef d'identification secrète K_t . Le module sécurisé MSO peut donc calculer la clef de session K_t' à partir de la clef d'identification K_t et du nombre aléatoire $Rnd1$.

Le module sécurisé MS0 dispose encore du nombre aléatoire Rnd2 qu'il a fourni précédemment à la carte de jeu. A partir de ces deux nombres Rnd2 et Kt', le module de sécurité MS0 calcule à nouveau un certificat C' en appliquant une seconde fois l'algorithme DES.

En vérifiant que le certificat C calculé par la carte correspond au certificat C' recalculé par son module de sécurité, l'organe central peut authentifier le message de donnée reçu.

Notons que la clé de session Kt' et le certificat C sont recalculés à chaque certification de message désirée. On évite ainsi que une machine pirate du réseau obtienne l'accès à la base de donnée ou à la mémoire de la carte en recopiant une certification précédente.

Après avoir effectué une ou plusieurs de ces vérifications, l'organe central 1 envoie un signal d'accord qui peut être crypté ou encodé. Avec un tel signal d'accord, le joueur peut utiliser sa carte de jeu CJ1, effectuer des mises, des opérations de jeu et recharger sa carte avec ses gains.

Dans ces deux premiers modes de réalisation, on a vu que la carte a une fonction d'identification, son numéro Id permettant à l'organe central 1 ou à la machine de jeu de la reconnaître voire de reconnaître le joueur dans certaines applications de fidélisation de clientèle. De plus, la carte a une fonction de porte-monnaie, le solde d'unités de valeur étant stocké dans la carte et connu essentiellement par la carte, la recopie de solde dans l'organe central 1 servant aux fins de vérification.

Selon un troisième mode de réalisation, la fonction porte-monnaie n'est plus assurée par la carte mais par l'organe central de gestion lui-même. La carte

ne comporte alors aucune donnée relative au solde du joueur mais uniquement des données d'identification, telles que le numéro d'identification Id, plusieurs clefs Kta, Ktb, Ktc d'authentification et éventuellement des informations sur le joueur. Les données de solde S1 des unités de valeur sont alors uniquement stockées dans la base de données BD de l'organe central de gestion 1. Ce compte d'unités de valeur se trouve par exemple dans la base de données sous le numéro d'identification Id1.

Lors d'une opération de jeu, le numéro d'identification Id de la carte CJ1 est envoyé à l'organe central de gestion 1 via les moyens de liaison 123 du réseau. Le numéro d'identification Id peut être envoyé directement par la machine de jeu 200 ou par son transcripteur 210 s'il a été mémorisé par la machine ou par son transcripteur. Le numéro d'identification Id peut aussi être lu sur la carte et envoyé à l'organe central de gestion 1 par le transcripteur 210 à chaque opération de jeu.

Après vérification du numéro d'identification Id, l'organe central de gestion 1 consulte la base de données BD et envoie à la machine de jeu 200 le solde S1 des unités de valeur affecté à la carte CJ1.

De préférence le transfert des données de solde d'unités de valeur est effectué avec un certificat selon le protocole de sécurisation des échanges de données présenté précédemment.

Un avantage de ce troisième mode de réalisation est que les montants mis en jeu sont stockés dans l'organe central de gestion 1, ce qui évite toute mémorisation de valeur au niveau des cartes de jeu.

Selon ce troisième mode de réalisation, il est donc prévu de stocker, dans la base de données des

moyens centralisés de gestion, les données représentatives du solde des valeurs débitées et/ou créditées afin d'éviter une fraude à partir d'une carte à puce.

5 Le contrôle consiste simplement dans ce troisième mode de réalisation à vérifier le numéro d'identification Id de la carte de jeu CJ1 avec une clé d'identification Kt1 lue dans la base de données BD de l'organe central de gestion 1 afin de contrôler
10 l'intégrité de la carte.

Avec ces trois modes de réalisation de l'invention on a vu qu'on peut avantageusement contrôler l'intégrité des cartes de jeu utilisées sur les machines de jeu.

15 De plus, en mettant en oeuvre des moyens de sécurisation des échanges de données, l'invention permet avantageusement de vérifier l'intégrité d'un système formé par les cartes de jeu, le réseau de machines de jeu et la base de données de l'organe
20 central de gestion, l'intégrité d'un des trois éléments du système, soit une carte de jeu, soit le réseau, soit la base de données étant vérifiée à l'aide des deux autres éléments.

25 L'invention prévoit en effet un système apte à mettre en oeuvre le procédé selon l'invention.

Un tel système comporte une pluralité de machines de jeu, chaque machine étant pourvue d'un transcripteur apte à débiter des unités de valeur d'une carte de jeu, les machines étant reliées en réseau avec un organe
30 central de gestion par l'intermédiaire de moyens de liaison.

Selon l'invention, les données représentatives des opérations de jeu effectuées avec une carte à puce sur une machine de jeu sont stockées en mémoire de la carte

de jeu et parallèlement dans une base de données prévue dans l'organe central de gestion.

Les données stockées sont notamment les données d'identification de la carte et le solde ou les soldes
5 successifs d'unités de valeur débitées et/ou créditées avec la carte.

Des moyens de contrôle tels qu'un programme d'ordinateur effectuant l'authentification du numéro d'identification de la carte ou la comparaison des
10 valeurs de solde stockées sur la carte et dans la base ou encore la certification des données échangées sont prévus afin de vérifier l'intégrité du système.

De préférence, pour sécuriser les échanges de données sur le réseau, il est prévu qu'un module de
15 sécurisation calcule un certificat d'authentification à partir de données secrètes stockées en mémoire du module et en ce que les moyens de contrôle vérifient que le certificat d'authentification calculé par le module de sécurisation correspond au certificat
20 d'authentification calculé par la carte de jeu ou par un autre module de sécurisation.

De tels modules de sécurisation MS0, MS1 peuvent être disposés dans les cartes du jeu CJ1, CJ2, ..., CJn, ou au niveau des transcodeurs 10, 110, 210,
25 210', 210'', 210''', 310, des machines de jeu 200, 200', 200'', 200''', de l'organe central de gestion 1 ou même sur les moyens de liaison 123 du réseau.

On peut en particulier prévoir plusieurs modules ou des moyens répartis de sécurisation au sein du
30 réseau. Chaque transcodeur 10, 210, 210', 210'', 210''', ou chaque interface 11, 120, 120', 120'', 120''' comprend par exemple un module de sécurisation de sorte que les échanges de données sur les moyens de liaison 123 son accompagnés de "certificat d'authentification.

Par exemple le transcripteur 10 émetteur ajoute à son message son certificat qui est authentifié par le transcripteur 210 destinataire avant d'être transmis à la machine 200 correspondante.

5 D'autres variantes de réalisation, avantages et caractéristiques de l'invention, apparaîtront à l'homme du métier sans sortir du cadre des revendications ci-après.

REVENDICATIONS

1. Procédé sécurisé de contrôle de transferts d'unités de valeur entre une pluralité de cartes de jeu (CJ, CJ1, CJ2, CJn) et une pluralité de machines de jeu (200, 200', 200'', 200''', 300, 300', 300''), chaque machine étant connectée à un transcripteur (210) de données sur carte de jeu (CJ2), les machines étant reliées en réseau sécurisé avec un organe central de gestion (1) par l'intermédiaire de moyens de liaison (123), le procédé comportant des étapes consistant, au cours d'une opération de jeu, à :
- lire des données en mémoire d'une carte de jeu, notamment un numéro d'identification (Id) de la carte (CJ1) et/ou des données (S, Op1, Op2, Opx) représentatives des unités de valeur débitées et/ou créditées au cours des opérations de jeu précédentes, le procédé étant caractérisé en ce qu'il comporte des étapes consistant à :
 - échanger des données entre la machine (200) et une base de données (BD) de l'organe central de gestion (1) par l'intermédiaire des moyens de liaison (123) du réseau sécurisé, notamment des données représentatives de solde (S) des unités de valeur et/ou le numéro d'identification (Id) de la carte ; et,
 - vérifier que les données en mémoire de la carte de jeu (CJ1) correspondent aux données de la base de données (BD) afin de contrôler l'intégrité d'un système constitué par une telle carte, une telle machine, le réseau et l'organe central de gestion.
2. Procédé selon la revendication 1, caractérisé par une étape préliminaire aux opérations de jeu, consistant à :

5 - inscrire, dans la base de données (BD) de l'organe central de gestion (1) et dans la mémoire d'une carte de jeu (CJ1), des données représentatives d'un solde (S, S1) initial d'unités de valeur lors d'une opération préliminaire de chargement de la carte.

3. Procédé selon l'une des revendications précédentes, caractérisé par une étape consistant, au cours d'une opération de jeu, à :

10 - inscrire, dans la base de données (BD) de l'organe central de gestion (1), des données représentatives du solde (S1) des unités de valeur de la carte de jeu (CJ1).

15 4. Procédé selon l'une des revendications précédentes, caractérisé par une étape consistant, au cours d'une opération de jeu, à :

- recevoir les données représentatives du solde (S1) des unités de valeur à partir de l'organe central de gestion (1) afin d'éviter une fraude à partir d'une carte (CJ2) ou d'une machine de jeu (200).

20 5. Procédé selon l'une des revendications précédentes, caractérisé en ce que l'étape de vérification consiste à :

25 - vérifier les données représentatives de solde (S) des unités de valeur lues en mémoire de la carte de jeu (CJ1) par rapport aux données (S1) lues dans la base de données (BD) afin de contrôler l'intégrité de la carte de jeu (CJ1).

30 6. Procédé selon l'une des revendications précédentes, caractérisé en ce que l'étape de vérification consiste à :

- vérifier le numéro d'identification (Id) de la carte de jeu (CJ1) avec une clé d'identification (Kt1) lue dans la base de données (BD) de l'organe central de

gestion (1) afin de contrôler l'intégrité de la carte de jeu (CJ1).

7. Procédé selon l'une des revendications précédentes caractérisé en ce que le réseau comporte en outre des
5 moyens de sécurisation (MS0), le procédé comportant une étape supplémentaire consistant à :

- prévoir que les moyens de sécurisation (MS0) du réseau calculent un certificat d'authentification (C') à partir de données secrètes (Kt, Kt') en mémoire des
10 moyens de sécurisation.

8. Procédé selon la revendication 7, caractérisé par une étape supplémentaire consistant à :

- lire un certificat d'authentification (C) calculé par la carte de jeu (CJ1) à partir de données
15 secrètes (Kt, Kt1) en mémoire de la carte.

9. Procédé selon la revendication 8 caractérisé en ce que l'étape de vérification consiste à :

- vérifier que le certificat d'authentification (C) calculé par la carte de jeu (CJ1) correspond au
20 certificat d'authentification (C') calculé par les moyens de sécurisation (MS0) du réseau.

10. Procédé selon l'une des revendications précédentes caractérisé en ce que le réseau comporte en outre des
25 moyens de sécurisation répartis (MS0, MS1), le procédé comportant des étapes supplémentaires consistant à :

- prévoir que des premiers moyens de sécurisation (MS0) du réseau calculent un premier certificat d'authentification (C') à partir de données secrètes (Kt, Kt') en mémoire des premiers moyens de
30 sécurisation (MS0), et

- prévoir que des seconds moyens de sécurisation (MS1) du réseau calculent un second certificat d'authentification à partir de données secrètes en mémoire des seconds moyens de sécurisation (MS1), et

- vérifier que le premier certificat d'authentification (C') calculé par les premiers moyens de sécurisation (MS0) du réseau correspond au second certificat d'authentification calculé par les seconds
5 moyens de sécurisation (MS1) du réseau.
11. Procédé selon l'une des revendications 7 à 10 caractérisé en ce que les données (Id, S) échangées entre la machine (200) et la base de données (BD) de l'organe central de gestion (1) sont accompagnées d'un
10 certificat d'authentification (C, C').
12. Procédé selon l'une des revendications précédentes caractérisé en ce que des moyens de sécurisation (MS1) sont associés au transcripteur (T, 10, 110, 210) de données sur carte de jeu (CJ1) afin de contrôler
15 l'intégrité d'une telle carte.
13. Procédé selon l'une des revendications précédentes caractérisé en ce que des moyens de sécurisation (MS1) sont associés à une machine de jeu (T, 200, 300).
14. Procédé selon l'une des revendications précédentes
20 caractérisé en ce que des moyens de sécurisation sont associés aux moyens de liaison du réseau.
15. Procédé selon l'une des revendications précédentes caractérisé en ce que des moyens de sécurisation (MS0) sont associés à l'organe central de gestion (1) afin de
25 contrôler l'intégrité du réseau.
16. Système sécurisé de contrôle de transferts d'unités de valeur entre une pluralité de cartes de jeu (CJ) et une pluralité de machines de jeu (200, 300), chaque machine étant pourvue d'un transcripteur (210,
30 310) apte à débiter des unités de valeur d'une carte de jeu (CJ), les machines étant reliées en réseau sécurisé avec un organe central de gestion (1) par l'intermédiaire de moyens de liaison (123), une carte de jeu (CJ1) stockant en mémoire des données (S, Op1,

Op2, Opx) représentatives d'opérations de jeu effectuées, notamment des données d'identification (Id) de la carte et des données représentatives de solde (S) des unités de valeurs débitées et/ou créditées au cours des opérations de jeu précédentes, caractérisé en ce que l'organe central de gestion (1) comporte une base de données (BD) stockant parallèlement en mémoire les données (S1, Op101, Op102, Op10x) représentatives des opérations de jeu effectuées, notamment les données d'identification (Id1, Id2, Idn) des cartes et les données représentatives des soldes (S1, S2, Sn) des unités de valeur débitées et/ou créditées au cours des opérations de jeu précédentes et en ce que des moyens de contrôle (BD) vérifient que, pour une carte identifiée, les données de la base (BD) et les données de la carte (CJ1) correspondent, notamment que les données (S, S1) représentatives du solde d'unités de valeur correspondent, afin de vérifier l'intégrité du système.

17. Système sécurisé selon la revendication 16, caractérisé en ce que la carte de jeu (CJ1) calcule un certificat d'authentification (C) à partir de données secrètes (Kt, Kt') stockées en mémoire de la carte (CJ1).

18. Système sécurisé selon la revendication 16 ou la revendication 17, caractérisé en ce qu'il comporte en outre au moins un module de sécurisation (MS0, MS1), le module de sécurisation calculant un certificat d'authentification (C') à partir de données secrètes (Kt, Kt') stockées en mémoire du module (MS0) et en ce que les moyens de contrôle (MS0) vérifient que le certificat d'authentification (C') calculé par le module de sécurisation correspond au certificat

d'authentification (C') calculé par la carte de jeu ou par un autre module de sécurisation (MS1).

19. Système sécurisé selon la revendication 18, caractérisé en ce qu'un module de sécurisation (MS1) est disposé dans le transcripteur (T, 10, 210, 310).
20. Système sécurisé selon l'une des revendications 18 et 19, caractérisé en ce qu'un module de sécurisation (MS0) est disposé dans une machine de jeu (200).
21. Système sécurisé selon l'une des revendications 18 à 20, caractérisé en ce qu'un module de sécurisation est disposé sur les moyens de liaison du réseau.
22. Système sécurisé selon l'une des revendications 18 à 21, caractérisé en ce qu'un module de sécurisation (MS0) est disposé dans l'organe central de gestion (1).
23. Procédé ou système sécurisé selon l'une des revendications précédentes caractérisé en ce qu'une carte de jeu est une carte à puce.
24. Procédé ou système sécurisé selon l'une des revendications précédentes caractérisé en ce qu'une carte de jeu est une carte sans contact.
25. Procédé ou système sécurisé selon l'une des revendications précédentes caractérisé en ce qu'une carte de jeu est une carte bancaire.

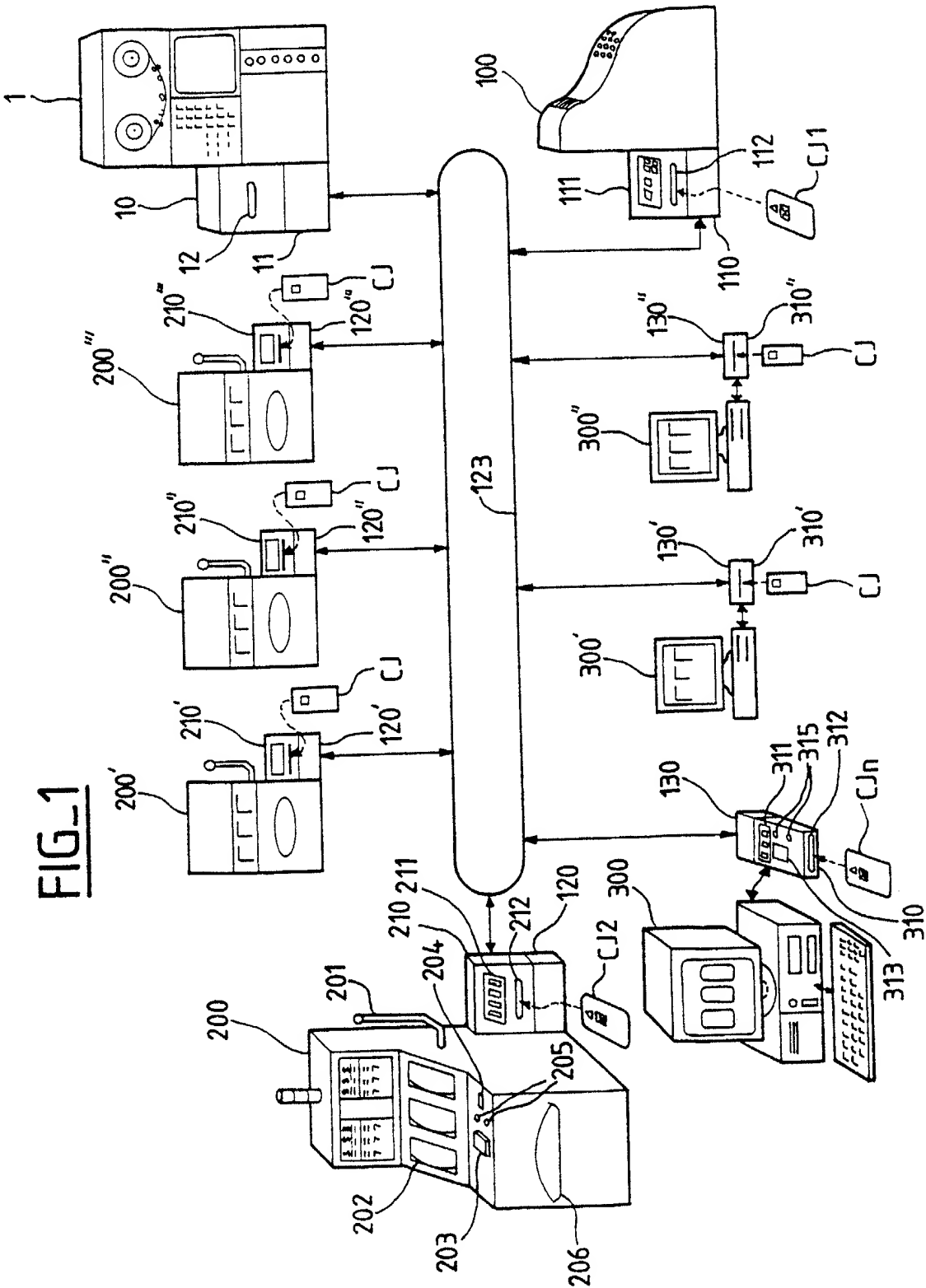


FIG-2

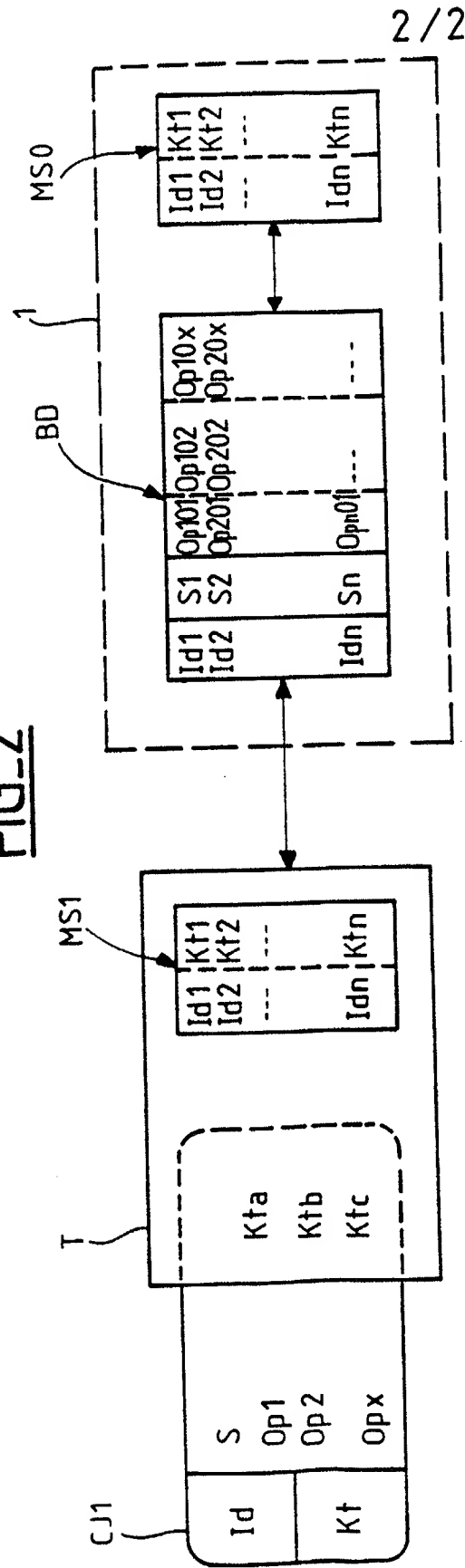
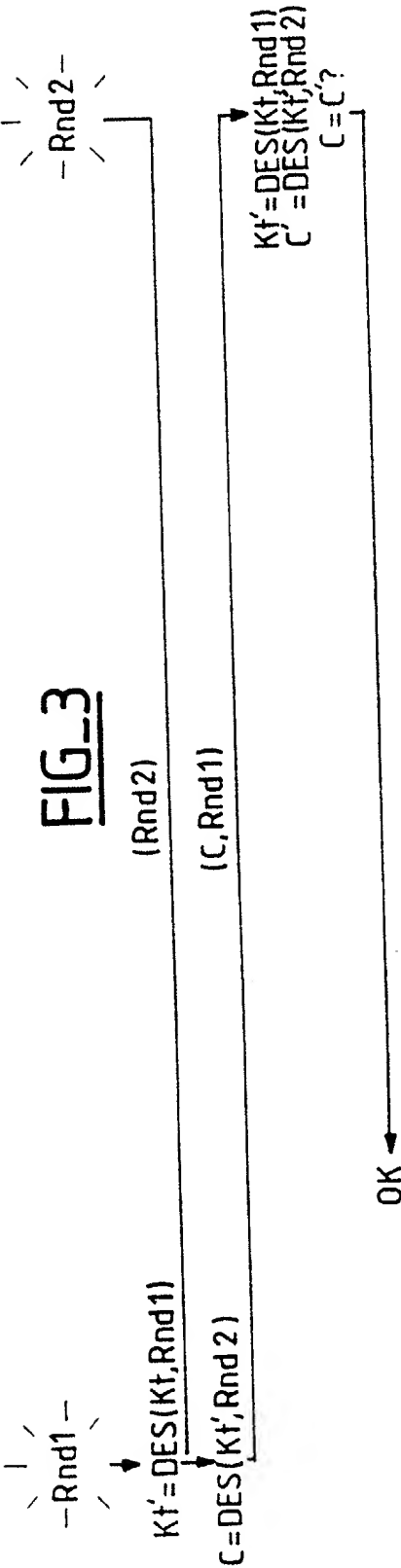


FIG-3



INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 98/00582

A. CLASSIFICATION OF SUBJECT MATTER

IPC 6 G07F17/32 G07F7/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 93 17403 A (NSM) 2 September 1993 see abstract; claims 13-24; figures see page 6, paragraph 2 - page 9, paragraph 1	1-5, 16, 23
Y	DE 44 27 039 A (GIESECKE & DEVRIENT) 1 February 1996 see abstract; claims; figures 1, 2 see column 3, line 32 - column 4, line 41	1-5, 16, 23
A	EP 0 589 545 A (BALLY GAMING INTERNATIONAL) 30 March 1994 see abstract; claims; figure see column 4, line 8 - column 8, line 56	1-6, 16, 23
A	WO 96 08798 A (GEMPLUS) 21 March 1996 see abstract; claims; figures	1, 2, 6-23
-/--		



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"Z" document member of the same patent family

Date of the actual completion of the international search

21 July 1998

Date of mailing of the international search report

31/07/1998

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

David, J

INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 98/00582

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 762 333 A (TEXAS INSTRUMENTS) 12 March 1997 ----	
A	EP 0 619 564 A (PITNEY BOWES) 12 October 1994 ----	
A	WO 97 02547 A (KONINKLIJKE PTT NEDERLAND) 23 January 1997 -----	

INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No

PCT/FR 98/00582

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9317403 A	02-09-1993	DE 4205791 A AT 132992 T DE 59301417 D EP 0628192 A US 5557086 A	02-09-1993 15-01-1996 22-02-1996 14-12-1994 17-09-1996
DE 4427039 A	01-02-1996	EP 0696021 A	07-02-1996
EP 0589545 A	30-03-1994	US 5371345 A AU 660561 B AU 4623393 A CA 2105925 A	06-12-1994 29-06-1995 24-03-1994 18-03-1994
WO 9608798 A	21-03-1996	FR 2724748 A AU 3475695 A ZA 9507809 A	22-03-1996 29-03-1996 07-05-1996
EP 0762333 A	12-03-1997	JP 9297862 A	18-11-1997
EP 0619564 A	12-10-1994	US 4802218 A EP 0619563 A EP 0619565 A AT 116778 T AT 160456 T AT 160039 T AU 605443 B AU 7961287 A CA 1320578 A CA 1326911 A CA 1335839 A CA 1296809 A DE 3750958 D DE 3750958 T DE 3752138 D DE 3752138 T DE 3752146 D DE 3752146 T DK 228888 A EP 0294397 A EP 0740275 A	31-01-1989 12-10-1994 12-10-1994 15-01-1995 15-12-1997 15-11-1997 10-01-1991 24-03-1988 20-07-1993 08-02-1994 06-06-1995 03-03-1992 16-02-1995 08-06-1995 11-12-1997 26-03-1998 02-01-1998 09-04-1998 17-06-1988 14-12-1988 30-10-1996

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 98/00582

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0619564 A		FI 882047 A, B,	02-05-1988
		JP 1500863 T	23-03-1989
		JP 2661932 B	08-10-1997
		NO 300660 B	30-06-1997
		WO 8801818 A	10-03-1988
		US 4864618 A	05-09-1989
		US 4900904 A	13-02-1990
		US 4900903 A	13-02-1990
WO 9702547 A	23-01-1997	NL 1000741 C	08-01-1997
		AU 6613096 A	05-02-1997
		EP 0836730 A	22-04-1998
		NO 976151 A	03-03-1998

RAPPORT DE RECHERCHE INTERNATIONALE

de internationale No

PCT/FR 98/00582

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 G07F17/32 G07F7/08

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 6 G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	WO 93 17403 A (NSM) 2 septembre 1993 voir abrégé; revendications 13-24; figures voir page 6, alinéa 2 - page 9, alinéa 1 ---	1-5, 16, 23
Y	DE 44 27 039 A (GIESECKE & DEVRIENT) 1 février 1996 voir abrégé; revendications; figures 1, 2 voir colonne 3, ligne 32 - colonne 4, ligne 41 ---	1-5, 16, 23
A	EP 0 589 545 A (BALLY GAMING INTERNATIONAL) 30 mars 1994 voir abrégé; revendications; figure voir colonne 4, ligne 8 - colonne 8, ligne 56 --- -/--	1-6, 16, 23



Voir la suite du cadre C pour la fin de la liste des documents



Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

21 juillet 1998

Date d'expédition du présent rapport de recherche internationale

31/07/1998

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

David, J

RAPPORT DE RECHERCHE INTERNATIONALE

De. de internationale No

PCT/FR 98/00582

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 96 08798 A (GEMPLUS) 21 mars 1996 voir abrégé; revendications; figures ----	1,2,6-23
A	EP 0 762 333 A (TEXAS INSTRUMENTS) 12 mars 1997 ----	
A	EP 0 619 564 A (PITNEY BOWES) 12 octobre 1994 ----	
A	WO 97 02547 A (KONINKLIJKE PTT NEDERLAND) 23 janvier 1997 -----	

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Requête internationale No

PCT/FR 98/00582

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9317403 A	02-09-1993	DE 4205791 A	02-09-1993
		AT 132992 T	15-01-1996
		DE 59301417 D	22-02-1996
		EP 0628192 A	14-12-1994
		US 5557086 A	17-09-1996
DE 4427039 A	01-02-1996	EP 0696021 A	07-02-1996
EP 0589545 A	30-03-1994	US 5371345 A	06-12-1994
		AU 660561 B	29-06-1995
		AU 4623393 A	24-03-1994
		CA 2105925 A	18-03-1994
WO 9608798 A	21-03-1996	FR 2724748 A	22-03-1996
		AU 3475695 A	29-03-1996
		ZA 9507809 A	07-05-1996
EP 0762333 A	12-03-1997	JP 9297862 A	18-11-1997
EP 0619564 A	12-10-1994	US 4802218 A	31-01-1989
		EP 0619563 A	12-10-1994
		EP 0619565 A	12-10-1994
		AT 116778 T	15-01-1995
		AT 160456 T	15-12-1997
		AT 160039 T	15-11-1997
		AU 605443 B	10-01-1991
		AU 7961287 A	24-03-1988
		CA 1320578 A	20-07-1993
		CA 1326911 A	08-02-1994
		CA 1335839 A	06-06-1995
		CA 1296809 A	03-03-1992
		DE 3750958 D	16-02-1995
		DE 3750958 T	08-06-1995
		DE 3752138 D	11-12-1997
		DE 3752138 T	26-03-1998
		DE 3752146 D	02-01-1998
		DE 3752146 T	09-04-1998
		DK 228888 A	17-06-1988
		EP 0294397 A	14-12-1988
		EP 0740275 A	30-10-1996

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Do. de internationale No

PCT/FR 98/00582

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0619564 A		FI 882047 A, B,	02-05-1988
		JP 1500863 T	23-03-1989
		JP 2661932 B	08-10-1997
		NO 300660 B	30-06-1997
		WO 8801818 A	10-03-1988
		US 4864618 A	05-09-1989
		US 4900904 A	13-02-1990
		US 4900903 A	13-02-1990
WO 9702547 A	23-01-1997	NL 1000741 C	08-01-1997
		AU 6613096 A	05-02-1997
		EP 0836730 A	22-04-1998
		NO 976151 A	03-03-1998

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Pierre

RECU le
02 NOV. 1998

PCT

Expéditeur: le BUREAU INTERNATIONAL

AVIS INFORMANT LE DEPOSANT DE LA
COMMUNICATION DE LA DEMANDE
INTERNATIONALE AUX OFFICES DESIGNES
(règle 47.1.c), première phrase, du PCT).

Destinataire:
NONNENMACHER, Bernard
Gemplus S.C.A.
Z.I. Athelia III
Voie Antiope
F-13705 La Ciotat Cedex
FRANCE

ov

el

Date d'expédition (jour/mois/année) 22 octobre 1998 (22.10.98)		
Référence du dossier du déposant ou du mandataire GEM 362		
AVIS IMPORTANT		
Demande internationale no PCT/FR98/00582	Date du dépôt international (jour/mois/année) 20 mars 1998 (20.03.98)	Date de priorité (jour/mois/année) 11 avril 1997 (11.04.97)
Déposant GEMPLUS S.C.A. etc		

1. Il est notifié par la présente qu'à la date indiquée ci-dessus comme date d'expédition de cet avis, le Bureau International a communiqué, comme le prévoit l'article 20, la demande internationale aux offices désignés suivants:
AU,BR,CA,CN,EP,JP,KR,US

Conformément à la règle 47.1.c), troisième phrase, ces offices acceptent le présent avis comme preuve déterminante du fait que la communication de la demande internationale a bien eu lieu à la date d'expédition indiquée plus haut, et le déposant n'est pas tenu de remettre sa copie de la demande internationale à l'office ou aux offices désignés.

2. Les offices désignés suivants ont renoncé à l'exigence selon laquelle cette communication doit être effectuée à cette date:
MX,RU,SG,VN

La communication sera effectuée seulement sur demande de ces offices. De plus, le déposant n'est pas tenu de remettre de copie de la demande internationale aux offices en question (règle 49.1a-bis).

3. Le présent avis est accompagné d'une copie de la demande internationale publiée par le Bureau International le 22 octobre 1998 (22.10.98) sous le numéro WO 98/47113

RAPPEL CONCERNANT LE CHAPITRE II (article 31.2a) et règle 54.2)

Si le déposant souhaite reporter l'ouverture de la phase nationale jusqu'à 30 mois (ou plus pour ce qui concerne certains offices) à compter de la date de priorité, la demande d'examen préliminaire international doit être présentée à l'administration compétente chargée de l'examen préliminaire international avant l'expiration d'un délai de 18 mois à compter de la date de priorité.

Il appartient exclusivement au déposant de veiller au respect du délai de 18 mois.

Il est à noter que seul un déposant qui est ressortissant d'un Etat contractant du PCT lié par le chapitre II ou qui y a son domicile peut présenter une demande d'examen préliminaire international.

RAPPEL CONCERNANT L'OUVERTURE DE LA PHASE NATIONALE (article 22 ou 39.1))

Si le déposant souhaite que la demande internationale procède en phase nationale, il doit, dans le délai de 20 mois ou de 30 mois, ou plus pour ce qui concerne certains offices, accomplir les actes mentionnés dans ces dispositions auprès de chaque office désigné ou élu.

Pour d'autres informations importantes concernant les délais et les actes à accomplir pour l'ouverture de la phase nationale, voir l'annexe du formulaire PCT/IB/301 (Notification de la réception de l'exemplaire original) et le volume II du Guide du déposant du PCT.

Bureau International de l'OMPI 34, chemin des Colonnnettes 1211 Genève 20, Suisse	Fonctionnaire autorisé J. Zahra
no de télécopieur (41-22) 740.14.35	no de téléphone (41-22) 338.83.88
Formulaire PCT/IB/308 (juillet 1996)	

2267410

PCT

ORGANISATION MONDIALE DE LA PROPRIÉTÉ INTELLECTUELLE
Brevet international

DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIÈRE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 : **G07F 17/32, 7/08**

AI

(11) Numéro de publication internationale: **WO 98/47113**

(43) Date de publication internationale: **22 octobre 1998 (22.10.98)**

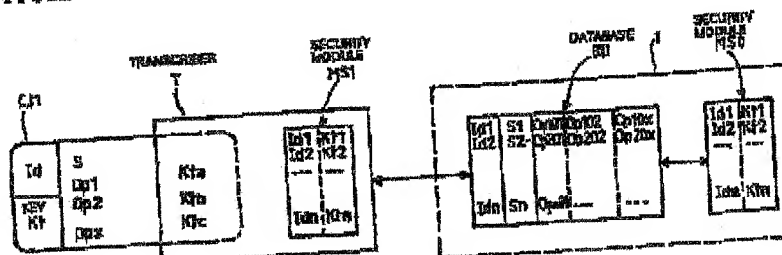
(21) Numéro de la demande internationale: **PCT/FR98/00582**(22) Date de dépôt international: **20 mars 1998 (20.03.98)**(30) Données relatives à la priorité: **97/04733 11 avril 1997 (11.04.97)**

FR

(71) Déposant (pour tous les Etats désignés sauf US): **GEMPLUS S.C.A. [FR/FR]; Avenue du Pic de Bastagne, Parc d'activités de Gémenos, F-13881 Gémenos Cedex (FR).**(72) Inventeurs; et
(73) Inventeurs/Déposants (US seulement): **ORLUS, Hervé [FR/FR]; 20, rue de la Graufortie, Zac Lou Cairé, F-13470 Carnoux en Provence (FR). FOGLINO, Jean-Jacques [FR/FR]; Les Terrasses de l'Audoubert, F-13790 Peynier (FR).**(74) Mandataire: **NONNENMACHER, Bernard; Gempius S.C.A., Z.I. Athélie III, Voie Andoche, F-13705 La Ciotat Cedex (FR).**(81) Etats désignés: **AU, BR, CA, CN, JP, KR, MX, RU, SG, US, VN, brevet européen (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).**

Publiée

Avec rapport de recherche internationale.

(54) Title: **SECURITY PROCEDURE FOR CONTROLLING THE TRANSFER OF VALUE UNITS IN A CHIP CARD GAMING SYSTEM**(54) Titre: **PROCEDURE SECURISEE DE CONTROLE DE TRANSFERT D'UNITES DE VALEUR DANS UN SYSTEME DE JEU A CARTES A PUCE**M-IDENTIFICATION
Op-ACCOUNT BALANCE

(57) Abstract

The invention concerns slot machines, such as jackpot or black jack and other casino gambling machines. The machines are designed to operate with gaming cards (CH), such as chip cards, and are connected by network to a central management unit (1). The invention is characterised in that the central management unit comprises a database (BD), wherein are stored data corresponding to those stored on the gaming cards such data concerning the gamster and card identification data (Id) and data (S, Op1, Op2) concerning the account balance stored in the card (CH). The procedure consists in verifying the card data with respect to the central management unit database to ensure the integrity of such a gambling machine system operating with chip cards or contactless cards.

(57) Abrégé

L'invention concerne les machines à sous, type jack-pot, black-jack, et autres machines de jeu d'argent de casino. Il est prévu que les machines de jeu fonctionnent avec des cartes de jeu (CJT), type carte à puce, et sont reliées en réseau avec un organe central de gestion (1). L'invention prévoit que l'organe central de gestion comporte une base de données (BD), dans laquelle sont stockées des informations correspondantes à celles stockées sur les cartes de jeu comme des informations sur le joueur ainsi que des données (Id) d'identification des cartes et des données (S, Op1, Op2) renseignant sur le solde de la valeur stockée dans la carte (CJT). Une vérification des données de la carte par rapport aux données de la base de l'organe central de gestion permet d'assurer l'intégrité d'un tel système de machines de jeu fonctionnant avec des cartes à puce ou des cartes sans contact.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	ME	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce	ML	Mali	TR	Turquie
BG	Bulgarie	HR	Croatie	MN	Mongolie	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MR	Mauritanie	UA	Ukraine
BR	Brazili	IL	Israël	MW	Malawi	UG	Ouganda
BV	Bélarus	IS	Islande	MX	Mexique	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	NE	Niger	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NL	Pays-Bas	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norvège	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NZ	Nouvelle-Zélande	ZW	Zimbabwe
CI	Côte d'Ivoire	KH	République populaire démocratique de Corée	PL	Pologne		
CM	Cameroun	LC	République de Cuba	PT	Portugal		
CN	Chine	LI	Kazakhstan	RO	Roumanie		
CU	Cuba	LT	Lituanie	RU	Fédération de Russie		
CZ	République tchèque	LV	Lettonie	SD	Soudan		
DE	Allemagne	LI	Liechtenstein	SE	Suède		
DK	Danemark	LK	Sri Lanka	SG	Singapour		
EE	Estonie	LR	Libéria				

WO 98/47113

PCT/FR98/00582

PROCEDURE SECURISEE DE CONTROLE DE TRANSFERT D'UNITES
DE VALEUR DANS UN SYSTEME DE JEU A CARTE A PUCE

5 La présente invention concerne le domaine des machines à sous, telles que les dispositifs de jack-pot et les autres dispositifs de jeux d'argent individuels du type de ceux que l'on trouve dans les casinos.

10 Elle concerne plus particulièrement des machines à sous permettant d'enregistrer des mises et des gains avec des cartes de jeu. Les cartes de jeu sont du type carte à puce ou carte sans contact. Les cartes de jeu peuvent être dédiées à cette utilisation suivant l'exemple des cartes téléphoniques. Elles sont
15 avantageusement constituées par des cartes bancaires, permettant de transférer des sommes d'argent directement sur la machine à sous.

20 La présente demande vise un procédé et un système de contrôle de transfert d'unités de valeur entre une pluralité de cartes de jeu et une pluralité de machines de jeu, chaque machine étant connectée à un transcripteur de données sur cartes de jeu apte à
créditer et/ou à débiter des unités de valeur en mémoire d'une carte de jeu.

25 Un objectif général du contrôle de transfert d'unités de valeurs entre cartes de jeu et machines de jeu est d'éviter toute malversation financière à l'aide de telle cartes.

30 On connaît déjà des systèmes de gestion pour des machines de jeu équipées de lecteurs de cartes à puce, adaptés à la gestion d'un parc de machines de jeux disposées dans des sites relativement fermés et contrôlés comme les casinos. Ces systèmes sont adaptés à un tel environnement, car il font l'objet de contrôles et de réglementations importants, peu

WO 98/47113

2

PCT/TR98/00582

susceptibles de permettre des fraudes sur les transactions de jeux utilisant des cartes à puce.

Le document EP-A-0 360 613 décrit par exemple un système de transfert de données entre carte à puce et une pluralité de machines avec des moyens de transmission et de stockage des données machine dans la carte à puce. Un tel système permet d'effectuer un relevé des opérations de jeu avec une carte de collecte stockant une liste des opérations de jeux effectuées dans un but comptable ou fiscal.

Un inconvénient d'un tel système est qu'on ne peut pas contrôler toutes les opérations de jeu effectuées, sauf à relever toutes les machines avec la carte de collecte, ce qui occasionne des manipulations fastidieuses.

D'autre part, devant la demande croissante du public, il est envisagé d'installer des machines de jeu dans des sites moins protégés que les casinos comme des salles de jeux privées ou des bars, voire même dans des lieux d'habitation privés comme le domicile des joueurs.

Il apparaît clairement qu'une telle dispersion des machines de jeu pose d'importants problèmes de sécurité des transactions suite aux opérations de jeu.

Un but de l'invention est de permettre un développement des machines de jeu fonctionnant avec des cartes à puce dans des lieux non protégés.

Un autre but de l'invention est de renforcer l'intégrité des systèmes de machines de jeux fonctionnant avec des cartes de jeu.

L'invention prévoit que les machines de jeu sont reliées en réseau avec un organe central de gestion. Selon l'invention on a prévu que l'organe central de gestion comporte une base de données, dans laquelle

WO 98/47113

3

PCT/FR98/00582

5 sont stockées des informations correspondantes à celles
stockées sur les cartes de jeu comme des informations
sur le joueur ainsi que des données d'identification
des cartes et des données renseignant sur le solde de
la valeur stockée dans la carte. Une vérification des
données de la carte par rapport aux données de la base
de l'organe central de gestion permet d'assurer
l'intégrité d'un tel système de machines de jeu
fonctionnant avec des cartes à puce ou des cartes sans
10 contact.

L'invention prévoit ainsi un procédé sécurisé de
contrôle de transferts d'unités de valeur entre une
pluralité de cartes de jeu et une pluralité de machines
de jeu, chaque machine étant connectée à un
15 transcripteur de données sur carte de jeu, les machines
étant reliées en réseau sécurisé avec un organe central
de gestion par l'intermédiaire de moyens de liaison, le
procédé comportant des étapes consistant, au cours
d'une opération de jeu, à :

20 - lire des données en mémoire d'une carte de jeu,
notamment un numéro d'identification de la carte et des
données représentatives des unités de valeur débitées
et/ou créditées au cours des opérations de jeu
précédentes,

25 - échanger des données entre la machine et une base
de données de l'organe central de gestion par
l'intermédiaire des moyens de liaison du réseau
sécurisé, notamment des données représentatives de
solde des unités de valeur et/ou le numéro
d'identification de la carte ; et,

30 - vérifier que les données en mémoire de la carte
de jeu correspondent aux données de la base de données
afin de contrôler l'intégrité d'un système constitué

WO 98/47113

4

PCT/FR98/00582

par une telle carte, une telle machine, le réseau et l'organe central de gestion.

L'invention prévoit avantageusement des moyens de sécurisation qui permettent d'authentifier les messages de données échangées sur le réseau, c'est-à-dire de signer de tels messages.

L'invention prévoit en outre un système sécurisé de contrôle de transferts d'unités de valeur entre une pluralité de cartes de jeu et une pluralité de machines de jeu, chaque machine étant pourvue d'un transcripteur apta à débiter des unités de valeur d'une carte de jeu, les machines étant reliées en réseau sécurisé avec un organe central de gestion par l'intermédiaire de moyens de liaison, une carte de jeu stockant en mémoire des données représentatives d'opérations de jeu effectuées, notamment des données d'identification de la carte et des données représentatives de solde des valeurs débitées et/ou créditées au cours des opérations de jeu précédentes, caractérisé en ce que l'organe central de gestion comporte une base de données stockant parallèlement en mémoire les données représentatives des opérations de jeu effectuées, notamment les données d'identification des cartes et les données représentatives des soldes des valeurs débitées et/ou créditées au cours des opérations de jeu précédentes et en ce que des moyens de contrôle vérifient que, pour une carte identifiée, les données de la base et les données de la carte correspondent, notamment que les données représentatives du solde correspondent, afin de vérifier l'intégrité du système.

Un module de sécurisation pour l'authentification des messages de données peut avantageusement être prévu dans le réseau, au niveau d'un transcripteur, d'une

WO 98/47113

5

PCT/FR98/00582

machine, de l'organe central, ou même des moyens de liaison du réseau.

L'invention sera mieux comprise à la lecture de la description et des dessins qui suivent, donnés uniquement à titre d'exemples non limitatifs ; sur les
5 dessins annexés :

- la figure 1 représente un système sécurisé de contrôle de transfert d'unités de valeurs entre une pluralité de cartes de jeu et une pluralité de machines
10 de jeu apte à mettre en oeuvre l'invention ;

- la figure 2 représente un schéma d'échange et de vérification des données selon l'invention ; et,

- la figure 3 représente un calcul de certificat d'authentification par des moyens de sécurisation selon
15 l'invention.

Sur la figure 1 on a représenté un système sécurisé de machines de jeu tel que proposé par l'invention, et qui comprend une ou plusieurs machines de jeu 200,
20 200', 200" et 200'''.

Une telle machine de jeu 200, semblable aux machines à sous que l'on trouve dans les casinos
25 dispose d'un monnayeur électronique 210 que l'on appellera par la suite transcripteur de données sur carte de jeu CJ.

Le transcripteur de données sur carte 210 est relié à l'électronique de la machine 200, par exemple par une
liaison série de type RS 485. La machine et le lecteur
comportent des interfaces entrée-sortie adaptées à
cette liaison.

De façon classique, la machine est équipée d'un
30 écran d'affichage 211 qui permet aux joueurs de savoir à tout instant quel est le solde dont il dispose pour jouer et le montant des mises et des gains réalisés.

WO 98/47113

6

PCT/FR98/00582

La machine 200 qui a été représentée peut bien sûr être une machine à monnayeur électronique exclusivement, mais aussi une machine à double monnayeur, c'est-à-dire une machine qui comporte outre ce monnayeur électronique, un monnayeur à pièces (ou à jetons) symbolisé par la référence 201.

Dans le cas d'une machine à double monnayeur, le joueur aura la possibilité de jouer avec des pièces ou jetons et de se faire restituer ses gains uniquement sous la forme de pièces.

Les cartes de jeu CJ représentées sous forme de cartes à puce comportent une mémoire morte effaçable électriquement, par exemple une mémoire de type EEPROM.

Il peut s'agir également de cartes à puce comportant un microprocesseur, une mémoire de programmes et une mémoire de travail de type RAM.

Ces cartes à puce peuvent également être des cartes à chargement d'unités de type rechargeable. Ces cartes comportent pour cela une mémoire électriquement programmable du genre boullier.

En outre les cartes de jeu peuvent être constituées par des cartes sans contact, la carte comportant un circuit intégré à mémoire et microprocesseur, et un circuit électronique de transmission de données sans contact électrique. On peut par exemple utiliser un transpondeur tel que décrit dans la demande de brevet FR - 96 16061.

La réalisation des machines de jeu 200 et leur connexion à des transpositeurs de données sur cartes de jeu ne sera pas détaillée ici. Des exemples de réalisations de machines de jeu sont détaillés par exemple dans la demande de brevet FR - 96 10031 dont la description est incorporée à la présente.

WO 98/47113

7

PCT/FR98/00582

Afin de contrôler les opérations de jeux et les transactions avec les cartes, il est prévu de relier les machines 200, 200', 200'', 200''' en réseau, avec un organe central de gestion représentés sous la référence 1 à la figure 1. Les machines du réseau sont reliées à l'organe central de gestion 1 par des moyens de liaison 123. Comme représentées à la figure 1, les machines 200, 200', 200'', 200''' peuvent également être reliées entre elles par le réseau.

Les moyens de liaison 123 sont constitués dans le cas d'un réseau local comme celui d'un casino par une liaison locale. La liaison locale est par exemple une liaison série de type RS 485, un bus de liaison parallèle, une fibre optique, une liaison radio ou tout autre support de transmission.

Dans le cas d'un réseau joignant des salles de jeu dispersées, les moyens de liaisons peuvent être constitués par des canaux de transmission propres au réseau ou par des lignes téléphoniques.

Pour établir des liaisons téléphoniques, le réseau comporte des modulateurs-démodulateurs de type MODEM 120, 120', 120'' et 120''', disposés en interface entre les moyens de liaison 123 et une machine de jeux 200, 200', 200'', 200''' respectivement.

L'organe central de gestion 1 est constitué par exemple d'un ordinateur central relié également aux moyens de liaison 123 par un MODEM 101 de façon à faire partie du réseau.

Sur la figure 1 on a représenté des moyens de liaison 123 sous la forme schématique d'une ligne annulaire à laquelle les machines de jeux 200, 200', 200'' et 200''' sont connectées. Les machines sont ainsi reliées entre elles et à l'organe central de gestion 1.

WO 98/47113

8

PCT/FR98/00582

La liaison peut cependant prendre toutes sortes de formes équivalentes.

5 Dans le cas de liaisons téléphoniques, les machines sont reliées individuellement aux moyens centralisés de gestion, les machines n'étant pas nécessairement reliées entre elles. Le MODEM 101 des moyens de gestion
1 peut comporter avantageusement un standard de plusieurs lignes téléphoniques.

10 L'utilisation de liaisons téléphoniques présente l'avantage de permettre d'étendre le réseau au lieu d'habitation des joueurs. Les machines de jeux sont de préférence constituées par des ordinateurs personnels 300 et 300' de type PC. Les machines peuvent ainsi être
15 connectées chacune à un transcripteur de données sur carte de jeu 310 ou 310' intégrant de préférence un MODEM 130 ou 130', par exemple du type "GEMTEL" commercialisé par la demanderesse.

Le réseau utilisé peut être notamment un réseau de communication ouvert du type "INTERNET".

20 Il est prévu en outre que le système et le réseau comportent au moins un terminal de chargement représenté à la figure 1 sous forme d'une caisse enregistreuse 100. Le terminal de chargement 100 comporte alors un transcripteur 110. Le terminal 100 et
25 le transcripteur 110 sont alors reliés au réseau par l'intermédiaire d'un MODEM 111 connecté aux moyens de liaison 123.

Classiquement, il est prévu que les cartes à puce dédiées aux jeux sont des cartes non-rechargeables, à
30 l'instar des cartes téléphoniques, et elles sont fabriquées et chargées uniquement par un organisme central.

Dans une application avec des cartes non-rechargeables, il est prévu que la base de données BD

WO 98/47113

9

PCT/TR98/00582

des moyens centralisés de gestion 1 dispose des soldes S1, S2, ..., Sn initiaux des valeurs créditées sur les cartes CJ1, CJ2, ..., CJn avant leur mise en circulation.

5 Cependant, selon une variante avantageuse, il est prévu que les cartes sont rechargées en unités de valeurs par l'intermédiaire de terminaux de chargement.

10 En pratique, ce terminal peut être celui d'un caissier du casino. De façon alternative, on peut prévoir une multitude de terminaux de chargements disposés dans des débits de tabac ou dans d'autres commerces accessibles aux joueurs.

15 Ainsi lorsqu'un joueur désire obtenir la délivrance d'un crédit, il donne sa carte de jeu CJ1 à l'opérateur habilité à utiliser le terminal 100 qui insère cette carte dans la partie transcripteur 110 de ce terminal 100 et qui au moyen du clavier de la caisse va rentrer le montant du crédit que désire avoir le joueur. Ce montant est transféré au transcripteur 110 qui

20 enregistre alors sur la carte à puce CJ1 l'information significative correspondant au crédit désiré par le joueur.

25 Selon l'invention, le terminal de rechargement peut alors communiquer à l'organe central de gestion 1, par l'intermédiaire des moyens de liaison du réseau 123, les données lues sur la carte à recharger, notamment son numéro d'identification Id et son solde S d'unités de valeur. La vérification du numéro d'identification Id de la carte de jeu CJ1 peut être faite directement

30 par le terminal de rechargement 100 ou par son transcripteur de données 110 ou de manière alternative par l'organe central de gestion 1. L'invention prévoit ainsi une étape préliminaire aux opérations de jeu, consistant à inscrire dans la base de données de

WO 98/47113

10

PCT/FR98/00582

l'organe central de gestion 1 et dans la mémoire d'une carte de jeu CJ1, des données représentatives d'une valeur de solde initial lors d'une opération préliminaire de chargement de la carte CJ1.

5 Selon la première alternative, il est prévu comme visible à la figure 2 que le terminal de rechargement ou son transcripteur T dispose des clefs d'identification secrètes Kt1, Kt2, ..., Ktn de toutes les cartes de jeu CJ1, CJ2, ..., CJn en circulation.

10 Ces clés secrètes sont de préférence stockées dans un module de sécurisation MS1 comportant une mémoire et une unité de calcul, les données stockées n'étant pas accessibles de l'extérieur. Le terminal 100 vérifie alors que l'identification Id1 de la carte à puce CJ1

15 est correcte avec la clef Kt1 correspondante, en appliquant un algorithme d'authentification ou de cryptage selon les méthodes connues.

Selon la seconde alternative, cette authentification de la carte est effectuée au niveau de

20 l'organe central de gestion 1, les numéros d'identification Id1, Id2, ..., Idn et les clefs d'authentification correspondantes Kt1, Kt2, ..., Ktn étant stockées dans la base de données BD de l'organe central de gestion ou de préférence dans un module de

25 sécurité MSD similaire à MS1. Cette seconde alternative présente l'avantage d'éviter toute dissémination des clefs d'authentification secrètes.

L'invention prévoit en outre un échange de données entre le terminal et l'organe central de gestion

30 portant sur les données stockées dans la base de données de l'organe central de gestion 1. De préférence, cet échange de données est accompagné d'un certificat d'authentification. Un protocole de sécurisation permettant d'émettre de tels certificats

WO 98/47113

11

PCT/FR98/00582

sera détaillé ci-après. Ce protocole évite
avantageusement qu'une machine parasite du réseau ne
crédite abusivement la base de données. Le terminal T
peut ainsi communiquer le solde S des valeurs débitées
5 et/ou créditées précédemment sur la carte de jeu CJ1 à
l'organe central de gestion 1. Après avoir authentifié
le numéro d'identification Id1 de la carte ou le
certificat accompagnant les données de solde, on peut
ainsi vérifier que le solde S inscrit en mémoire de la
10 carte de jeu CJ1 correspond bien au solde S1 stocké
dans la base de données BD. Si la vérification est
positive, il est prévu que l'organe central de gestion
1 émet un signal d'accord pour le rechargement de la
carte CJ1 par le terminal et le transcripteur T. En cas
15 de vérification négative, une procédure ou un signal
d'alerte peuvent être mis en oeuvre au niveau de
l'organe central de gestion 1, ou au niveau du terminal
de chargement. Dans un réseau de machines à sous de
casino par exemple, le caissier pourra être alerté par
20 le terminal de chargement afin de découvrir l'origine
d'un tel dysfonctionnement. Dans un réseau plus étendu,
on peut prévoir que la carte CJ1 soit avalée par le
transcripteur T du terminal afin d'enquêter sur le
dysfonctionnement.

25 On peut prévoir en outre que la base de données ou
la mémoire des cartes de jeu CJ comportent des
informations sur le joueur, par exemple sur son âge,
ses habitudes de jeu pour des applications de
fidélisation des joueurs, de remise de parties
30 gratuites, etc.

Nous allons présenter maintenant des protocoles de
contrôle de transferts d'unités de valeur au cours
d'opérations de jeu effectuées avec le procédé ou le
système selon l'invention.

PCT/TR98/00582

WO 98/47113

12

5 Au début des opérations de jeu, le transcripteur de données sur carte 210 de la machine de jeu lit le numéro d'identification en mémoire de la carte de jeu CJ1. Comme exposé précédemment au vu de la figure 2, ce
10 numéro d'identification Id est de préférence authentifié par un module de sécurité MS1 prévu dans la transcripteur T. Le numéro Id peut éventuellement être communiqué à l'organe central de gestion 1 en vue d'authentifier la carte CJ1 avec la clef
15 d'identification Kt1 contenue dans le module de sécurité MS0. Cette étape d'identification est de préférence effectuée une seule fois pour plusieurs opérations de jeu avec la même carte sur la même machine, la machine ou le terminal mémorisant éventuellement ce numéro d'identification Id pour les
opérations suivantes.

A chaque opération de jeu suivante, le solde S des unités de valeur affecté au joueur est revu à la suite des mises ou des gains réalisés.

20 Selon un premier mode de réalisation de l'invention, il est prévu de communiquer simplement à l'organe central de gestion 1 des données relatives à l'opération de jeu effectuée, notamment le nouveau solde d'unités de valeur obtenu au cours de cette
25 opération de jeu. L'organe central de gestion 1 peut ainsi stocker la liste des opérations effectuées, sous forme d'une liste des crédits ou des débits successifs enregistrés sur la carte CJ1. Cette liste des
30 opérations Op101, Op102, ... , Op10x est par exemple enregistrée dans la base de données BD sous le numéro d'identification Id1 de la carte CJ1 en cours d'utilisation.

La recopie du solde S1 ou des opérations Op101, Op102, ... , Op10x dans la base de données BD de

WO 98/47113

13

PCT/TR98/00582

l'organe central de gestion 1 sert alors à établir un relevé comptable des opérations ou à effectuer des vérifications fiscales. Un tel historique des opérations permet également lors d'une vérification d'une carte falsifiée de mesurer l'étendue de la fraude.

Selon un deuxième mode de réalisation de l'invention, il est prévu une étape supplémentaire consistant à vérifier que les données en mémoire de la carte CJI et les données de la base de données BD correspondent afin de contrôler l'intégrité d'un système constitué par une telle carte CJI, une telle machine 200, le réseau 123 et l'organe central de gestion 1.

Deux types de vérification peuvent être prévues, la vérification pouvant porter sur le numéro d'identification Id ou sur le solde S de la carte.

La vérification du numéro d'identification Id1 de la carte CJI est effectuée avec une clé d'identification Kt1 comme on l'a vu précédemment. Selon ce deuxième mode de réalisation, le numéro d'identification Id est communiqué à l'organe central 1 via les moyens de liaison 123 du réseau. L'organe central 1 stocke les clés d'identification Kt1, Kt2, ..., Ktn des cartes CJI, CJ2, ..., CJn en circulation, dans sa base de données BD ou de préférence dans un module de sécurisation MS0. Le module de sécurisation MS0 effectue ainsi les calculs d'identification en interne.

De plus, la vérification peut porter sur le solde d'unités de valeur de la carte CJI. Dans ce cas, le transcripteur T lit sur la carte les données de solde S des unités de valeur et les envoie à l'organe central de gestion 1 par l'intermédiaire des moyens de liaison

WO 98/47113

14

PCT/FR98/00582

du réseau 123. La vérification du solde S de la carte CJ1 est alors effectuée par rapport au solde S1 indiqué dans la base de données BD sous le numéro d'identification Id1. Si les deux soldes S et S1 correspondent, l'opération de jeu est autorisée par l'organe central de gestion 1.

Selon une autre alternative, la vérification peut porter sur la certification des données échangées à partir de la carte de jeu CJ1. Des algorithmes standardisés d'encryptage de données type algorithme DES permettant en effet de certifier les données numériques échangées entre la carte CJ1, le transcripteur T, la machine de jeu et l'organe central de gestion 1. Le cryptage et le décryptage du certificat accompagnant les données transmises n'est possible et cohérent que si on utilise une clé secrète.

Les algorithmes de cryptage de données de type DES comportent des séries de calculs complexes qui ne seront pas détaillés dans la présente.

Un exemple de mise en oeuvre d'algorithme DES sera exposé en considérant simplement que l'algorithme fournit un nombre crypté, appelé clef de session K', à partir d'un premier nombre donné, appelé clef d'identification K et d'un nombre aléatoire Rnd, selon l'exemple de la formule suivante :

$$K' = \text{DES}(K, \text{Rnd})$$

La complexité des algorithmes DES rend impossible la découverte d'une clef d'identification secrète K à partir de la clef de session K' et du nombre aléatoire Rnd.

La figure 3 montre un exemple d'application d'un algorithme DES. Il permet d'illustrer des moyens de sécurisation du réseau, en particulier la sécurisation

WO 98/47113

15

PCT/FR98/00582

des échanges de données effectuées via les moyens de liaison du réseau. La carte de jeu dispose dans une zone mémoire inaccessible d'au moins une clé d'identification secrète K_t . Le microprocesseur de la carte génère un nombre pseudo aléatoire $Rnd1$. A partir de ces deux nombres $Rnd1$ et K_t , l'algorithme DES mis en oeuvre par le microprocesseur calcule une clef de session K_t' .

Cette clef de session K_t' peut servir de certificat d'authentification et être envoyée avec le nombre aléatoire $Rnd1$ et les données à certifier. Cependant, pour rendre toute découverte des clefs impossible, il est prévu d'appliquer une seconde fois l'algorithme DES. Comme visible figure 1, la carte de jeu, organe émetteur du message à certifier, demande à l'organe destinataire, l'organe central 1 par exemple, de lui fournir un second nombre aléatoire $Rnd2$.

L'algorithme DES est à nouveau appliqué à la clef de session K_t' et au second nombre aléatoire $Rnd2$ par le microprocesseur de la carte pour calculer un certificat C.

Le message de données est alors envoyé à l'organe destinataire accompagné du certificat C et du nombre aléatoire $Rnd1$ calculés par la carte. Ainsi les clefs utilisées, en particulier la clef d'identification secrète K_t , ne sont pas échangées.

L'authentification du message de données est effectué en recalculant un certificat C' à partir des mêmes données. L'organe central de gestion 1 dispose dans son module sécurisé MSO de la clef d'identification secrète K_t . Le module sécurisé MSO peut donc calculer la clef de session K_t' à partir de la clef d'identification K_t et du nombre aléatoire $Rnd1$.

WD 98/47113

16

PCI/FR98/00582

Le module sécurisé MS0 dispose encore du nombre aléatoire Rnd2 qu'il a fourni précédemment à la carte de jeu. A partir de ces deux nombres Rnd2 et Kt', le module de sécurité MS0 calcule à nouveau un certificat C' en appliquant une seconde fois l'algorithme DES.

En vérifiant que le certificat C calculé par la carte correspond au certificat C' recalculé par son module de sécurité, l'organe central peut authentifier le message de donnée reçu.

Notons que la clé de session Kt' et le certificat C sont recalculés à chaque certification de message désirée. On évite ainsi que une machine pirate du réseau obtienne l'accès à la base de donnée ou à la mémoire de la carte en recopiant une certification précédente.

Après avoir effectué une ou plusieurs de ces vérifications, l'organe central 1 envoie un signal d'accord qui peut être crypté ou encodé. Avec un tel signal d'accord, le joueur peut utiliser sa carte de jeu CFI, effectuer des mises, des opérations de jeu et recharger sa carte avec ses gains.

Dans ces deux premiers modes de réalisation, on a vu que la carte a une fonction d'identification, son numéro Id permettant à l'organe central 1 ou à la machine de jeu de la reconnaître voire de reconnaître le joueur dans certaines applications de fidélisation de clientèle. De plus, la carte a une fonction de porte-monnaie, le solde d'unités de valeur étant stocké dans la carte et connu essentiellement par la carte, la recopie de solde dans l'organe central 1 servant aux fins de vérification.

Selon un troisième mode de réalisation, la fonction porte-monnaie n'est plus assurée par la carte mais par l'organe central de gestion lui-même. La carte

WO 98/47113

17

PCT/TR98/00582

ne comporte alors aucune donnée relative au solde du joueur mais uniquement des données d'identification, telles que le numéro d'identification Id, plusieurs clefs Kta, Ktb, Ktc d'authentification et éventuellement des informations sur le joueur. Les données de solde si des unités de valeur sont alors uniquement stockées dans la base de données BD de l'organe central de gestion 1. Ce compte d'unités de valeur se trouve par exemple dans la base de données sous le numéro d'identification Id1.

Lors d'une opération de jeu, le numéro d'identification Id de la carte CJI est envoyé à l'organe central de gestion 1 via les moyens de liaison 123 du réseau. Le numéro d'identification Id peut être envoyé directement par la machine de jeu 200 ou par son transcripteur 210 s'il a été mémorisé par la machine ou par son transcripteur. Le numéro d'identification Id peut aussi être lu sur la carte et envoyé à l'organe central de gestion 1 par le transcripteur 210 à chaque opération de jeu.

Après vérification du numéro d'identification Id, l'organe central de gestion 1 consulte la base de données BD et envoie à la machine de jeu 200 le solde si des unités de valeur affecté à la carte CJI.

De préférence le transfert des données de solde d'unités de valeur est effectué avec un certificat selon le protocole de sécurisation des échanges de données présenté précédemment.

Un avantage de ce troisième mode de réalisation est que les montants mis en jeu sont stockés dans l'organe central de gestion 1, ce qui évite toute mémorisation de valeur au niveau des cartes de jeu.

Selon ce troisième mode de réalisation, il est donc prévu de stocker, dans la base de données des

PCT/FR98/00582

WO 98/47113

18

moyens centralisés de gestion, les données représentatives du solde des valeurs débitées et/ou créditées afin d'éviter une fraude à partir d'une carte à puce.

5 Le contrôle consiste simplement dans ce troisième mode de réalisation à vérifier le numéro d'identification Id de la carte de jeu CJ1 avec une clé d'identification Kt1 lue dans la base de données BD de l'organe central de gestion 1 afin de contrôler
10 l'intégrité de la carte.

Avec ces trois modes de réalisation de l'invention on a vu qu'on peut avantageusement contrôler l'intégrité des cartes de jeu utilisées sur les machines de jeu.

15 De plus, en mettant en oeuvre des moyens de sécurisation des échanges de données, l'invention permet avantageusement de vérifier l'intégrité d'un système formé par les cartes de jeu, le réseau de machines de jeu et la base de données de l'organe
20 central de gestion, l'intégrité d'un des trois éléments du système, soit une carte de jeu, soit le réseau, soit la base de données étant vérifiée à l'aide des deux autres éléments.

L'invention prévoit en effet un système apte à
25 mettre en oeuvre le procédé selon l'invention.

Un tel système comporte une pluralité de machines de jeu, chaque machine étant pourvue d'un transcripteur apte à débiter des unités de valeur d'une carte de jeu, les machines étant reliées en réseau avec un organe
30 central de gestion par l'intermédiaire de moyens de liaison.

Selon l'invention, les données représentatives des opérations de jeu effectuées avec une carte à puce sur une machine de jeu sont stockées en mémoire de la carte

WO 98/47113

19

PCT/FR98/00582

de jeu et parallèlement dans une base de données prévue dans l'organe central de gestion.

Les données stockées sont notamment les données d'identification de la carte et le solde ou les soldes successifs d'unités de valeur débitées et/ou créditées avec la carte.

Des moyens de contrôle tels qu'un programme d'ordinateur effectuant l'authentification du numéro d'identification de la carte ou la comparaison des valeurs de solde stockées sur la carte et dans la base ou encore la certification des données échangées sont prévus afin de vérifier l'intégrité du système.

De préférence, pour sécuriser les échanges de données sur le réseau, il est prévu qu'un module de sécurisation calcule un certificat d'authentification à partir de données secrètes stockées en mémoire du module et en ce que les moyens de contrôle vérifient que le certificat d'authentification calculé par le module de sécurisation correspond au certificat d'authentification calculé par la carte de jeu ou par un autre module de sécurisation.

De tels modules de sécurisation MS0, MS1 peuvent être disposés dans les cartes du jeu CJ1, CJ2, ..., CJn, ou au niveau des transcodeurs 10, 110, 210, 210', 210'', 210''', 310, des machines de jeu 200, 200', 200'', 200''', de l'organe central de gestion 1 ou même sur les moyens de liaison 123 du réseau.

On peut en particulier prévoir plusieurs modules ou des moyens répartis de sécurisation au sein du réseau. Chaque transcodeur 10, 210, 210', 210'', 210''', ou chaque interface 11, 120, 120', 120'', 120''' comprend par exemple un module de sécurisation de sorte que les échanges de données sur les moyens de liaison 123 son accompagnés de "certificat d'authentification.

WO 98/47113

20

PCT/FR98/00582

Par exemple le transcripteur 10 émetteur ajoute à son message son certificat qui est authentifié par le transcripteur 210 destinataire avant d'être transmis à la machine 200 correspondante.

3 D'autres variantes de réalisation, avantages et caractéristiques de l'invention, apparaîtront à l'homme du métier sans sortir du cadre des revendications ci-après.

WO 98/47113

21

PCT/FR98/00582

REVENDICATIONS

1. Procédé sécurisé de contrôle de transferts d'unités de valeur entre une pluralité de cartes de jeu (CJ, CJ1, CJ2, CJn) et une pluralité de machines de jeu (200, 200', 200'', 200''', 300, 300', 300''), chaque machine étant connectée à un transcripteur (210) de données sur carte de jeu (CJ2), les machines étant reliées en réseau sécurisé avec un organe central de gestion (1) par l'intermédiaire de moyens de liaison (123), le procédé comportant des étapes consistant, au cours d'une opération de jeu, à :
- lire des données en mémoire d'une carte de jeu, notamment un numéro d'identification (Id) de la carte (CJ1) et/ou des données (S, Op1, Op2, Opx) représentatives des unités de valeur débitées et/ou créditées au cours des opérations de jeu précédentes, le procédé étant caractérisé en ce qu'il comporte des étapes consistant à :
 - échanger des données entre la machine (200) et une base de données (BD) de l'organe central de gestion (1) par l'intermédiaire des moyens de liaison (123) du réseau sécurisé, notamment des données représentatives de solde (S) des unités de valeur et/ou le numéro d'identification (Id) de la carte ; et,
 - vérifier que les données en mémoire de la carte de jeu (CJ1) correspondent aux données de la base de données (BD) afin de contrôler l'intégrité d'un système constitué par une telle carte, une telle machine, le réseau et l'organe central de gestion.
2. Procédé selon la revendication 1, caractérisé par une étape préliminaire aux opérations de jeu, consistant à :

- 5 - inscrire, dans la base de données (BD) de l'organe central de gestion (1) et dans la mémoire d'une carte de jeu (CJ1), des données représentatives d'un solde (S, S1) initial d'unités de valeur lors d'une opération préliminaire de chargement de la carte.
3. Procédé selon l'une des revendications précédentes, caractérisé par une étape consistant, au cours d'une opération de jeu, à :
- 10 - inscrire, dans la base de données (BD) de l'organe central de gestion (1), des données représentatives du solde (S1) des unités de valeur de la carte de jeu (CJ1).
4. Procédé selon l'une des revendications précédentes, caractérisé par une étape consistant, au cours d'une opération de jeu, à :
- 15 - recevoir les données représentatives du solde (S1) des unités de valeur à partir de l'organe central de gestion (1) afin d'éviter une fraude à partir d'une carte (CJ2) ou d'une machine de jeu (200).
- 20 5. Procédé selon l'une des revendications précédentes, caractérisé en ce que l'étape de vérification consiste à :
- vérifier les données représentatives de solde (S) des unités de valeur lues en mémoire de la carte de jeu (CJ1) par rapport aux données (S1) lues dans la base de données (BD) afin de contrôler l'intégrité de la carte de jeu (CJ1).
- 25 6. Procédé selon l'une des revendications précédentes, caractérisé en ce que l'étape de vérification consiste à :
- 30 - vérifier le numéro d'identification (Id) de la carte de jeu (CJ1) avec une clé d'identification (Kt1) lue dans la base de données (BD) de l'organe central de

gestion (1) afin de contrôler l'intégrité de la carte de jeu (CJ1).

5 7. Procédé selon l'une des revendications précédentes caractérisé en ce que le réseau comporte en outre des moyens de sécurisation (MS0), le procédé comportant une étape supplémentaire consistant à :

- prévoir que les moyens de sécurisation (MS0) du réseau calculent un certificat d'authentification (C') à partir de données secrètes (Kt, Kt') en mémoire des
10 moyens de sécurisation.

8. Procédé selon la revendication 7, caractérisé par une étape supplémentaire consistant à :

- lire un certificat d'authentification (C) calculé par la carte de jeu (CJ1) à partir de données
15 secrètes (Kt, Kt1) en mémoire de la carte.

9. Procédé selon la revendication 8 caractérisé en ce que l'étape de vérification consiste à :

- vérifier que le certificat d'authentification (C) calculé par la carte de jeu (CJ1) correspond au
20 certificat d'authentification (C') calculé par les moyens de sécurisation (MS0) du réseau.

10. Procédé selon l'une des revendications précédentes caractérisé en ce que le réseau comporte en outre des moyens de sécurisation répartis (MS0, MS1), le procédé
25 comportant des étapes supplémentaires consistant à :

- prévoir que des premiers moyens de sécurisation (MS0) du réseau calculent un premier certificat d'authentification (C') à partir de données secrètes (Kt, Kt') en mémoire des premiers moyens de
30 sécurisation (MS0), et

- prévoir que des seconds moyens de sécurisation (MS1) du réseau calculent un second certificat d'authentification à partir de données secrètes en mémoire des seconds moyens de sécurisation (MS1), et

WO 98/47113

24

PCT/TR98/00582

- vérifier que le premier certificat d'authentification (C') calculé par les premiers moyens de sécurisation (MS0) du réseau correspond au second certificat d'authentification calculé par les seconds moyens de sécurisation (MS1) du réseau.
- 5 11. Procédé selon l'une des revendications 7 à 10 caractérisé en ce que les données (Id, S) échangées entre la machine (200) et la base de données (BD) de l'organe central de gestion (1) sont accompagnées d'un
- 10 certificat d'authentification (C, C').
12. Procédé selon l'une des revendications précédentes caractérisé en ce que des moyens de sécurisation (MS1) sont associés au transcripteur (T, 10, 110, 210) de données sur carte de jeu (CJ1) afin de contrôler
- 15 l'intégrité d'une telle carte.
13. Procédé selon l'une des revendications précédentes caractérisé en ce que des moyens de sécurisation (MS1) sont associés à une machine de jeu (T, 200, 300).
14. Procédé selon l'une des revendications précédentes caractérisé en ce que des moyens de sécurisation sont
- 20 associés aux moyens de liaison du réseau.
15. Procédé selon l'une des revendications précédentes caractérisé en ce que des moyens de sécurisation (MS0) sont associés à l'organe central de gestion (1) afin de
- 25 contrôler l'intégrité du réseau.
16. Système sécurisé de contrôle de transferts d'unités de valeur entre une pluralité de cartes de jeu (CJ) et une pluralité de machines de jeu (200, 300), chaque machine étant pourvue d'un transcripteur (210, 310) apte à débiter des unités de valeur d'une carte de
- 30 jeu (CJ), les machines étant reliées en réseau sécurisé avec un organe central de gestion (1) par l'intermédiaire de moyens de liaison (123), une carte de jeu (CJ1) stockant en mémoire des données (S, Op1,

WO 98/47113

25

PCT/FR98/00582

- Op2, OpX) représentatives d'opérations de jeu effectuées, notamment des données d'identification (Id) de la carte et des données représentatives de solde (S) des unités de valeurs débitées et/ou créditées au cours des opérations de jeu précédentes, caractérisé en ce que l'organe central de gestion (1) comporte une base de données (BD) stockant parallèlement en mémoire les données (S1, Op101, Op102, Op10X) représentatives des opérations de jeu effectuées, notamment les données d'identification (Id1, Id2, Idn) des cartes et les données représentatives des soldes (S1, S2, Sn) des unités de valeur débitées et/ou créditées au cours des opérations de jeu précédentes et en ce que des moyens de contrôle (BD) vérifient que, pour une carte identifiée, les données de la base (BD) et les données de la carte (CJ1) correspondent, notamment que les données (S, S1) représentatives du solde d'unités de valeur correspondent, afin de vérifier l'intégrité du système.
17. Système sécurisé selon la revendication 16, caractérisé en ce que la carte de jeu (CJ1) calcule un certificat d'authentification (C) à partir de données secrètes (Kt, Kt') stockées en mémoire de la carte (CJ1).
18. Système sécurisé selon la revendication 16 ou la revendication 17, caractérisé en ce qu'il comporte en outre au moins un module de sécurisation (MS0, MS1), le module de sécurisation calculant un certificat d'authentification (C') à partir de données secrètes (Kt, Kt') stockées en mémoire du module (MS0) et en ce que les moyens de contrôle (MS0) vérifient que le certificat d'authentification (C') calculé par le module de sécurisation correspond au certificat

WO 98/47113

26

PCT/FR98/0582

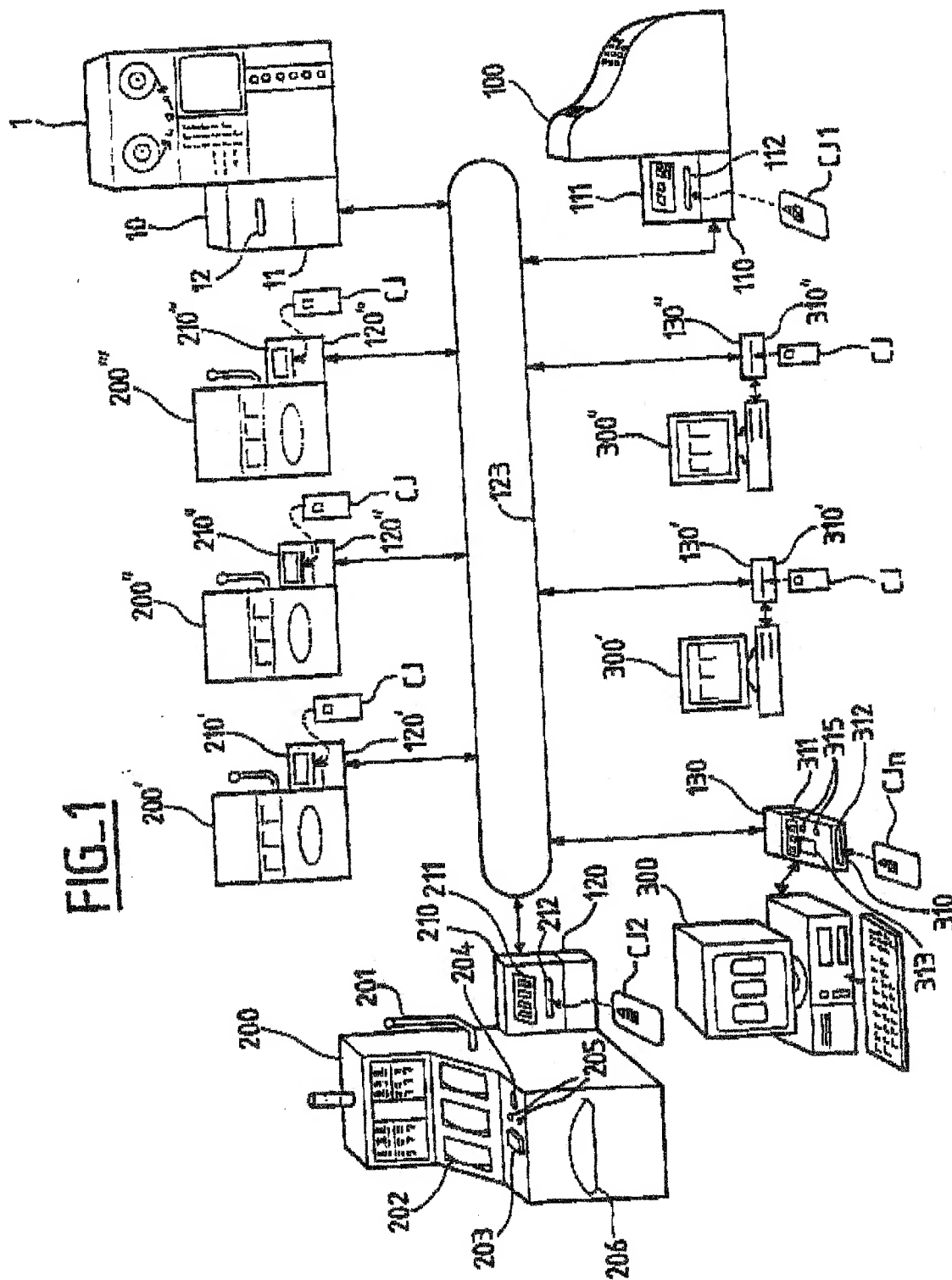
- d'authentification (C') calculé par la carte de jeu ou par un autre module de sécurisation (MS1).
19. Système sécurisé selon la revendication 18, caractérisé en ce qu'un module de sécurisation (MS1) est disposé dans le transcripteur (T, 10, 210, 310).
- 5 20. Système sécurisé selon l'une des revendications 18 et 19, caractérisé en ce qu'un module de sécurisation (MS0) est disposé dans une machine de jeu (200).
- 10 21. Système sécurisé selon l'une des revendications 18 à 20, caractérisé en ce qu'un module de sécurisation est disposé sur les moyens de liaison du réseau.
22. Système sécurisé selon l'une des revendications 18 à 21, caractérisé en ce qu'un module de sécurisation (MS0) est disposé dans l'organe central de gestion (1).
- 15 23. Procédé ou système sécurisé selon l'une des revendications précédentes caractérisé en ce qu'une carte de jeu est une carte à puce.
24. Procédé ou système sécurisé selon l'une des revendications précédentes caractérisé en ce qu'une carte de jeu est une carte sans contact.
- 20 25. Procédé ou système sécurisé selon l'une des revendications précédentes caractérisé en ce qu'une carte de jeu est une carte bancaire.

WO 98/47113

PCT/FR98/00582

1/2

FIG. 1



WO 98/47113

PCT/FR98/00582

2/2

FIG-2

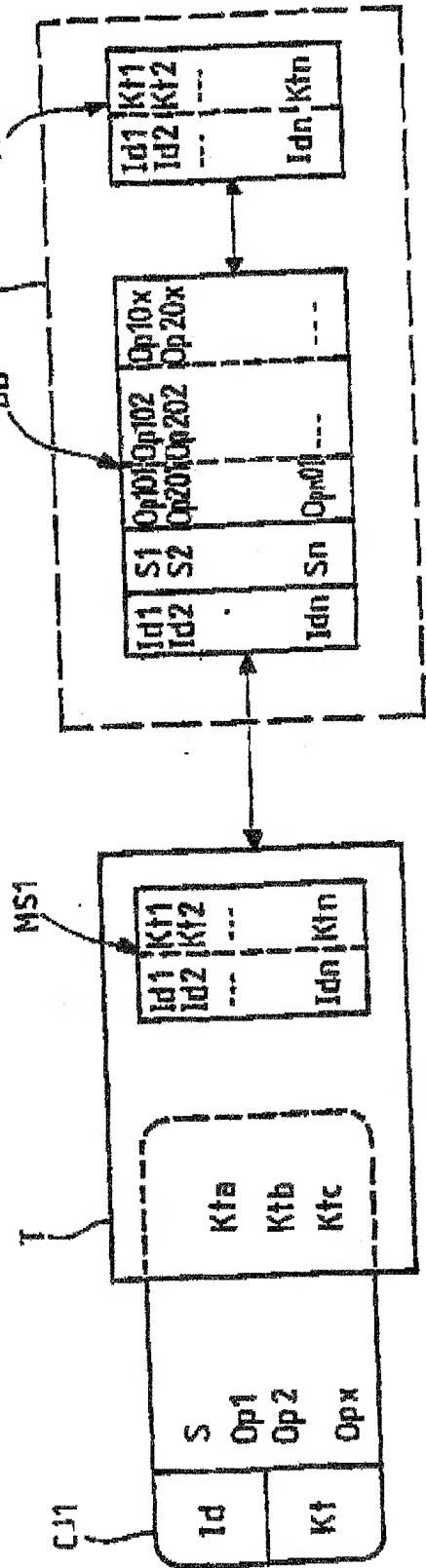


FIG-3

